S. Hrg. 109–304

VULNERABILITIES IN THE U.S. PASSPORT SYSTEM CAN BE EXPLOITED BY CRIMINALS AND TERRORISTS

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JUNE 29, 2005

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

22–199 PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

SUSAN M. COLLINS, Maine, *Chairman*

TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
TOM COBURN, Oklahoma
LINCOLN D. CHAFEE, Rhode Island
ROBERT F. BENNETT, Utah
PETE V. DOMENICI, New Mexico
JOHN W. WARNER, Virginia

JOSEPH I. LIEBERMAN, Connecticut
CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK DAYTON, Minnesota
FRANK LAUTENBERG, New Jersey
MARK PRYOR, Arkansas

MICHAEL D. BOPP, *Staff Director and Chief Counsel*
MICHAEL L. STERN, *Deputy Staff Director Director for Investigations*
JOYCE A. RECHTSCHAFFEN, *Minority Staff Director and Counsel*
KEVIN J. LANDY, *Minority Counsel*
TRINA D. TYRER, *Chief Clerk*

CONTENTS

Opening statements: Page
Senator Collins 1
Senator Lautenberg 4

WITNESSES

WEDNESDAY, JUNE 29, 2005

Jess T. Ford, Director, International Affairs and Trade, U.S. Government Accountability Office 5
Michael L. Johnson, Former Special Agent in Charge, Miami Field Office, Diplomatic Security Service, U.S. Department of State 8
Frank E. Moss, Deputy Assistant Secretary for Passport Services, Bureau of Consular Affairs, U.S. Department of State 19
Donna A. Bucella, Director, Terrorist Screening Center 21
Thomas E. Bush, III, Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation 22

ALPHABETICAL LIST OF WITNESSES

Bucella, Donna A.:
Testimony 21
Prepared statement 66
Bush, Thomas E., III:
Testimony 22
Prepared statement 69
Ford, Jess T.:
Testimony 5
Prepared statement 33
Johnson, Michael L.:
Testimony 8
Prepared statement 49
Moss, Frank E.:
Testimony 19
Prepared statement with attachments 54

APPENDIX

National Federation of Federal Employees, International Association of Machinists & Aerospace Workers, AFL–CIO, Local 1998, prepared statement 75
Reponses to questions for the Record for Mr. Moss from:
Senator Collins 90
Senator Lieberman 92

VULNERABILITIES IN THE U.S. PASSPORT SYSTEM CAN BE EXPLOITED BY CRIMINALS AND TERRORISTS

WEDNESDAY, JUNE 29, 2005

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS
Washington, DC.

The Committee met, pursuant to notice, at 9:31 a.m., in room SD–562, Dirksen Senate Office Building, Hon. Susan M. Collins, Chairman of the Committee, presiding.

Present: Senators Collins, Carper and Lautenberg.

Chairman COLLINS. The Committee will come to order. Good morning.

Before I begin the hearing today, I would like to express my deepest condolences to my friend and the Committee's Ranking Member, Senator Joe Lieberman. Senator Lieberman's mother passed away on Sunday, June 26, and he is unable to be with us today because he is observing the traditional Jewish 7-day period of mourning.

He is a co-requester with me of the GAO report on passport integrity, and I know that he is very concerned and interested in this subject. Senator Lieberman will be submitting questions for the record, and the record will remain open for 15 days in order to receive his materials as well as any others that the Committee Members wish to express, but I did want to explain the reason for Senator Lieberman's absence since he is such a diligent Member of this Committee.

OPENING STATEMENT OF CHAIRMAN COLLINS

Today the Committee will examine an issue that is central to our homeland security and that is the process for issuing a U.S. passport. As a new Government Accountability Office report makes clear, this process suffers from several vulnerabilities that could be exploited by terrorists and other criminals.

The U.S. passport is the gold card of travel documents. Governments worldwide treat it as unassailable proof of identity and of citizenship. It opens doors to international travel and expedites reentry to our country upon return. A fraudulent passport, however, can be a ticket to criminal activity and terrorism.

Technological improvements have made it extremely difficult to counterfeit or alter a U.S. passport, but it is less difficult to obtain an authentic passport by fraudulent means. A common fraud

scheme, accounting for 69 percent of cases detected last year, according to the State Department, is the use by an imposter of legitimate birth certificates and other identification documents belonging to another, in other words, identity theft. This scheme is often facilitated by organized fraud rings that can provide the imposter with suitable documents at a price. One such ring was recently uncovered smuggling hundreds of undocumented aliens from Ecuador and other South American countries into the United States for fees ranging from $12,000 to $14,000 each.

And there can be no doubt that fraudulent travel documents are essential to terrorists. As the 9/11 Commission found: "For terrorists, travel documents are as important as weapons. Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack." The Commission reported on many instances of al Qaeda's use of fraudulent foreign passports. In fact, the Commission's report documents an al Qaeda office of passports, which was charged with altering passports and other documents. Further, Jihadists were required to turn in their passports so that they could be recycled if they were killed. The Commission's report also describes how the operatives were trained to alter passports.

Around the world, in Australia, Indonesia, and South Africa, among other places, governments are investigating passport fraud with clear ties to terrorism. It is not surprising, therefore, that former Secretary of State Colin Powell described maintaining the integrity of the U.S. passport as "a critical component of our global effort to fight terrorism."

The GAO report that this Committee requested identifies a number of weaknesses in the State Department's efforts to detect and prevent passport fraud. These include insufficient staffing, training and oversight, and a lack of investigative resources dedicated to stopping passport fraud.

The GAO also raises troubling concerns about the State Department's ability to provide adequate oversight of nearly 7,000 passport acceptance facilities throughout the Nation, such as local post offices and courthouses which accept millions of passport applications each year. Last year the State Department had to stop accepting passport applications from one of these facilities when it learned that a corrupt county employee in New Jersey was aiding passport fraud by selling fraudulent birth certificates to illegal aliens.

Another fundamental flaw uncovered by GAO relates to an issue that Members of this Committee know all too well, and that is a profound lack of consistent and effective information sharing. It is inconceivable to me that in this post September 11 world we are still seeing examples of Federal agencies not sharing information that is vital to our security. The Terrorist Screening Center, which began operating in 2003, has a consolidated watch list database of known or suspected terrorists. The GAO reports that more than 20,000 names of Americans on this watch list were not incorporated into the State Department's database for passports. As the State Department and the Terrorist Screening Center have acknowledged, the failure to share this information means that a suspected terrorist could obtain a passport without alerting the appropriate authorities.

The fact that one of these individuals listed on the terrorist watch list has applied for a passport would almost certainly be significant for purposes of a counterterrorism investigation. Moreover, in an appropriate case, the Secretary of State could use her authority to deny a passport on the grounds that U.S. national's activities abroad are likely to cause serious damage to national security. But obviously, if an investigation is never triggered because the information is not shared, there is nothing that can be done.

The information-sharing problems go beyond the shadowy world of terrorism. The GAO investigation also revealed that the State Department name check system does not include the names of many Federal and State fugitives, individuals wanted for such crimes as murder, rape, robbery, and embezzlement. In fact, the CLASS system, the database used by the State Department, contains the names of only 50,000 of the more than 1.2 million Federal, State, and local fugitives in the United States. That is less than 5 percent.

To illustrate the problem, the GAO tested the names of 67 fugitives wanted for a variety of serious crimes, including murder, felonious assault, and child sex offenses. The GAO found that fewer than half were included in the CLASS database.

These fugitives not in CLASS could apply for and receive a U.S. passport in their own names and flee the country. In fact, one of the Federal fugitives, whose name GAO found was not in the CLASS system, did obtain a U.S. passport on May 12, 2004. This was 17 months after the FBI had listed this person in its database as wanted in connection with an $11 million telemarketing fraud. The fugitive was able to obtain an updated passport from an embassy abroad after his name was cleared in the State Department's database. This occurred despite the fact that there was an outstanding Federal warrant for his arrest.

Perhaps more alarming, one of the names tested by the GAO and found not to be in the State Department's database was that of Donald Eugene Webb. Mr. Webb, who is wanted in connection with the brutal murder of a police chief in Pennsylvania, appears on the FBI's Ten Most Wanted List. If someone like Mr. Webb could potentially apply for and receive a passport, the prospects of denying passports to possible terrorists are even more worrisome.

I am pleased that the Committee's investigation has spurred action on this subject. The State Department and the Terrorist Screening Center are making arrangements to share information on Americans on the terrorist watch list. The State Department has informed the Committee that it is near an agreement with the FBI's Violent Crimes Section to gain access to more fugitive data. The State Department has also taken steps recently to improve fraud detection training, enhance oversight, and dedicate more resources to fraud investigations. These developments are encouraging and welcome, but there is much more that remains to be done, and it disturbs me that these problems have continued for as long as they have.

Protecting the integrity of the U.S. passport is essential to protecting our citizens from those who would do us harm, whether they are terrorists or other criminals.

I look forward to hearing the testimony of our witnesses today as we seek to fortify our defenses.

Senator Lautenberg.

OPENING STATEMENT OF SENATOR LAUTENBERG

Senator LAUTENBERG. Thank you very much, Madam Chairman. Apparently you have set off an alarm through the bureaucracy that this is going to be under review and they had better get going. This morning I saw on television that there was talk between the FBI and the State Department. So you have already ruffled the feathers, and it is a good thing that you did.

You were kind enough, Madam Chairman, to mention Joe Lieberman, my dear friend, colleague here, the loss of his mother, and I join you in sending our condolences to him.

My guess is that the United States is the largest issuer of passports in the world of any of the countries, but if not the largest, certainly among the largest, and the fact that people on the terror watch list can get by, the criminals that we have identified here is outrageous. The funniest thing is that I have seen an example of the failure to connect with the terror watch list when it comes to issuing gun permits. We found out that they would almost never hit the terror watch list to see if someone was on that list, and how could we ignore that?

So it tells us something, I think, about the general policy or the general attitude that permits these people to get by and crack our security wall. It has always been important for us to maintain our Nation's borders, but it became absolutely vital in the wake of the terrorist attacks of September 11.

In order to keep track of who is crossing our borders, coming in and out of our country, we obviously rely on passports and visas. A valid U.S. passport is the ticket upon return to the country of citizens or those who would purport to be eligible passport recipients, that enables a person to enter our country and cross our borders at will. So any problem in the issuance of a passport is no mere bureaucratic hitch, it is a potential threat to our national security.

Passport fraud often is committed in connection with other crimes including those mentioned by the Chairman, including drug trafficking, money laundering, and smuggling of illegal aliens.

I know that various Federal agencies including DHS are working with the State Department to ensure that people who are not entitled to the U.S. passports do not get them. While that is comforting, it was alarming to learn that the State Department system for checking names on passports does not have access to the terrorist watch list or databases of wanted Federal and State fugitives.

Therefore a passport examiner would be unaware if a person seeking a passport was suspected of links to terrorism, even though our government has compiled a lengthy list of suspected terrorists. This looks like the classic example of the left hand not knowing what the right hand is doing, and I understand the State Department is now negotiating an agreement to make this information available, and we say here, the sooner the better.

The passport system also does not contain the names, as the Chairman said, of most Federal fugitives even though they are legally prohibited from receiving passports. GAO tested the names of a number of Federal fugitives and found that many were not in the State Department name check system. So it simply makes no sense. And as we approach the fourth anniversary of September 11, there is no longer any excuse for the bureaucracy standing in the way of national security.

Once again, thank you for calling this hearing, and I look forward to the thoughts of our witnesses.

Chairman COLLINS. Thank you, Senator.

I am delighted to welcome our first panel of witnesses this morning. Jess Ford is the Director of International Affairs and Trade at the U.S. Government Accountability Office and is the lead author of the report that we will discuss today. He has extensive experience in the areas of national security and international affairs, and I want to thank him for doing an excellent, thorough investigation.

Michael Johnson is the Former Special Agent in Charge of the Diplomatic Security Service's Miami Field Office, an office that I would note is the busiest office in the Nation for visa and passport fraud prosecutions. As Special Agent in Charge, Mr. Johnson was responsible for all Diplomatic Security Service operations in eight States. He, too, has extensive previous experience in running security programs at embassies around the world, and he currently serves in the Department of Commerce in the area of export enforcement.

I want to welcome both of you, and I thank you for joining us.

Mr. Ford, we will start with your testimony.

TESTIMONY OF JESS T. FORD,[1] DIRECTOR, INTERNATIONAL AFFAIRS AND TRADE, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. FORD. Thank you, Madam Chairman and Members of the Committee. I would like my full statement to be submitted in the record.

Chairman COLLINS. Without objection, all statements will be included in the record as well.

Mr. FORD. I am pleased to be here today to discuss our report on the State Department's efforts to strengthen U.S. passport fraud detection. Maintaining the integrity of the U.S. passport is essential to the State Department's effort to protect U.S. citizens from terrorists, criminals, and others.

The Department issued about 8.8 million passports in fiscal year 2004. Each year the State Department passport examiners refer tens of thousands of applicants they suspect may be fraudulent to their local Fraud Prevention Offices. In fiscal year 2004, the State Department's Diplomatic Security Service arrested about 500 individuals for passport fraud and about 300 of them were convicted.

Passport fraud is often intended to facilitate such crimes as illegal immigration, drug trafficking, and alien smuggling. Our report addresses three key issues: How passport fraud is committed, what key challenges the State Department faces in fraud detection ef-

[1] The prepared statement of Mr. Ford appears in the Appendix on page 33.

forts, and what effect new passport examiner performance standards could have on fraud detection. Today I am going to focus my discussion on the first two issues, and I will also discuss our recommendations to the State Department to respond to them.

We found that identity theft is the primary tactic used by individuals fraudulently applying for U.S. passports. Specifically, impostors using other people's legitimate birth and other identification documents accounted for about 69 percent of passport fraud detected in fiscal year 2004, while false claims of lost, stolen, and damaged passports and other methods accounted for the remaining 31 percent of cases.

According to the State Department's Bureau of Diplomatic Security, passport fraud is often committed in connection with other crimes, including narcotics trafficking, organized crime, money laundering, and alien smuggling. Fraudulently obtained passports can enable criminals to hide their movements and activities, and concerns exist that fraudulently obtained passports could be used to support terrorism. U.S. passports allow their holders to enter the United States with much less scrutiny than is given to foreign citizens and also allow visa-free passage into many countries around the world, providing obvious potential benefits to terrorists and criminals operating on an international scale.

Our report details a number of challenges to the State Department's passport fraud detection effort, including information sharing deficiencies, insufficient fraud prevention training, staffing and oversight, and investigative resources. These challenges make it more difficult to protect U.S. citizens from terrorists, criminals, and others who would harm the United States.

Specifically, the State Department does not currently receive information on U.S. citizens listed in the Terrorist Screening Center database, which is the Federal Government's consolidated terrorist watch list. Nor does the State Department routinely obtain information from the FBI on the names of individuals wanted on both Federal and State law enforcement authority warrants. Therefore, many of these individuals are not listed in the State Department's Consular Lookout and Support System name check database for passports, and they could obtain passports and travel internationally without the knowledge of appropriate authorities.

We tested the names of 67 different Federal and State fugitives, some wanted for serious crimes including murder and rape, and found that fewer than half were in the State Department system. To my left and right are some graphics that illustrate the issue.

The first poster on my right-hand side is a table that summarizes the listing of the 37 individuals that we found were not in the Consular Lookout System. As you can see in the chart, many of these individuals were wanted for serious crimes.[1]

To my left is a graphic of the most wanted poster individual in the FBI's Ten Most Wanted List, whom we found was not in the State Department system. You will note that Donald Eugene Webb is a dangerous individual. He is wanted for a brutal beating and murder of a police chief in Pennsylvania, and the FBI is offering a $100,000 reward for information leading to his capture.

[1] The chart referred to appears in the Appendix on page 34.

Also to my left is a wanted bulletin for James Stanley Eberhart, wanted for involvement in a telemarketing scheme which defrauded website investors out of $11 million.

As the Chairman noted in her opening statement, Mr. Eberhart obtained an updated U.S. passport 17 months after he had been listed in the FBI's Most Wanted List as an individual that they were interested in arresting.

Finally, the photograph to my right is a bulletin for William P. Fischer, wanted by the New York State Police for murdering his son and daughter's girlfriend.

These examples are merely illustrative of the many thousands of other wanted fugitives who are currently not listed in the State Department's name check system. Although the State Department, the Terrorist Screening Center, and the FBI have been made aware of this situation, they are now in the process of reaching an agreement to try to foreclose this vulnerability.

The State Department does not maintain a centralized electronic fraud prevention library that enables information sharing on fraud alerts, lost and stolen birth and naturalization certificates, counterfeit documents, and other fraud prevention resources.

We found that fraud prevention training is provided unevenly at the various passport issuing offices. Some examiners have not had formal fraud prevention training in years, and training and oversight of a passport acceptance agent operations are even more sporadic.

The State Department does not have any way of tracking whether many of the acceptance agent employees are receiving required training. It makes oversight visits in only a limited number of cases and it does not maintain records of all of the individuals in the acceptance facilities, posing significant fraud vulnerability.

Any effect that new passport fraud examiner performance standards may have had on the State Department's fraud detection efforts is unclear because the State Department has continued to adjust the standards. The State Department began implementing a new standard in January 2004 to make work processes and performance expectations more uniform nationwide. Passport examiner union representatives expressed concern that the new production quotas may require examiners to shortcut fraud detection efforts. However, in response to union and examiner concerns, the State Department eased the production standards during the rest of 2004 and made other modifications to the standards.

We made six recommendations to the State Department designed to improve the coordination and execution of passport fraud detection efforts. These included actions to improve and expedite information sharing specifically by ensuring that the State Department's Consular Lookout System for passports contains more comprehensive lists of individuals identified in the Terrorist Screening Center, as well as State and Federal fugitives.

We also recommended that they establish and maintain a central electronic fraud prevention library.

We are also recommending that the State Department consider designating additional positions for fraud prevention coordination and training in some domestic passport issuing offices.

We also recommended that they examine the impact of other workload-related issues related to fraud prevention and strengthen its fraud prevention training and acceptance agent oversight programs.

The State Department indicated in a response to our report that they were taking actions on most of the areas that we recommended.

This concludes my opening statement. I would be happy to answer any of your questions.

Chairman COLLINS. Thank you, Mr. Ford. Mr. Johnson.

TESTIMONY OF MICHAEL L. JOHNSON,[1] FORMER SPECIAL AGENT IN CHARGE, MIAMI FIELD OFFICE, DIPLOMATIC SECURITY SERVICE, U.S. DEPARTMENT OF STATE

Mr. JOHNSON. Good morning. I would like to thank Chairman Collins and all the other Members of the Committee for the opportunity to appear before you today. Passport fraud is a much misunderstood problem, and I am very pleased that the Committee is holding a hearing to discuss how it affects our country's homeland security, including the possibility that weaknesses in the passport issuance regime could be exploited by terrorists.

For the record, my name is Michael Johnson. I served in the State Department's Bureau of Diplomatic Security for 18 years. In 1999, I began serving in Diplomatic Security's Miami Field Office, rising to be a Special Agent in Charge in 2002 until I left at the end of 2004. I would like to add that while I am currently the Special Agent in Charge of the Miami Field Office of the Office of Export Enforcement for the Department of Commerce, I am not here today testifying on their behalf.

As you know, the State Department is the sole Executive Branch Department with the authority to issue passports to citizens of the United States. With this authority comes the responsibility to maintain the integrity of the U.S. passport. The Department's Bureau of Consular Affairs handles much of this responsibility, with the task of supporting its mission falling to the Bureau of Diplomatic Security's criminal investigative programs. Investigating passport fraud is just one of Diplomatic Security's responsibilities, which also include protecting the Secretary of State and high-ranking foreign dignitaries and officials visiting the United States, protecting U.S. embassies and consulates abroad, conducting personnel security investigations, and training foreign civilian law enforcement officers to protect their countries from terrorism.

As Special Agent in Charge of Diplomatic Security's Miami Field Office, I was charged with overseeing what has historically been Diplomatic Security's busiest field office. I believe this places me in a unique position to discuss efforts to combat passport fraud.

Possession of a U.S. passport is important because it allows an individual to prove two things: United States citizenship and identity. In fact, it is the only official government document that establishes both, making the U.S. passport the most widely accepted and versatile government-issued document in the United States. Most consider it the "gold standard" of all passports, and, as a result, it

[1] The prepared statement of Mr. Johnson appears in the Appendix on page 49.

can be used throughout the world to establish bank and credit accounts, to cash checks, apply for driver's licenses, welfare or unemployment, and any other activity requiring an individual to prove citizenship or identity.

There is a common misperception about passport fraud that I would like to clear up. First, passport fraud is not primarily committed to facilitate illegal immigration. In fact, the overwhelming majority of passport fraud cases involve applicants who are already in the United States. By fraudulently obtaining a U.S. passport, an unscrupulous individual will have the document that allows its holder to travel into and out of the United States freely, bypassing the border requirements for non-U.S. citizens.

It also provides ironclad proof of an individual's identity. The value of this document to an individual trying to conceal his identity or blend into American society is obvious, given the post September 11 scrutiny placed on non-U.S. citizens inside the United States. Stopping passport fraud should be at the core of strong border and homeland security procedures.

When discussing the problems posed by passport fraud, we should remember that the U.S. passport is an extraordinarily difficult document to counterfeit or to fraudulently modify. Unfortunately, the same cannot be said for a document used to establish eligibility for a passport. The threat to the passport comes when bogus versions of these documents, called breeder documents, are used in the passport application process to falsely establish an applicant's citizenship or nationality and proof of identity. Key among these breeder documents are bogus birth certificates. Weaknesses in these documents can provide unscrupulous individuals a back door method of acquiring a U.S. passport.

Despite the challenge posed to the integrity of the U.S. passport, I do not believe that enough is being done within the Department of State to protect this vitally important document. For example, in my experience, Diplomatic Security Service thinks of itself primarily as a security service and tends to view passport fraud as a less important part of its mission. Because it is not its main priority, sufficient resources are not dedicated to fighting passport fraud.

One way to solve this problem would be to assign additional civil service Diplomatic Security special agents to field offices for whom they would investigate passport fraud on a permanent basis. This would give them the time needed to develop sufficient expertise to effectively combat passport fraud and would develop a cadre of agents with the expertise to take down the fraud rings that are attacking the integrity of the U.S. passport.

Another significant obstacle in combatting passport fraud is that Diplomatic Security lacks an analytic capacity. During my service in the DSS, I found that there was simply no institutional capacity to spot and understand trends, analyze information gained from operations, and share intelligence across the DSS and other law enforcement organizations. The lack of such an intelligence capacity cripples DSS's ability to identify and dismantle organizations across the world that are involved in the manufacture and sale of counterfeit documents used to illegally enter and/or remain in the United States.

I again want to thank the Committee for holding this hearing, and I am now prepared to answer your questions.

Chairman COLLINS. Thank you, Mr. Johnson. You made an interesting comment that the passport fraud that you have seen was not primarily to facilitate illegal immigration and that the value of having a U.S. passport is that it allows the holder to conceal his true identity. Based on your considerable experience, how easy do you think it would be for a terrorist to obtain a fraudulent passport?

Mr. JOHNSON. I think it would be relatively easy, unfortunately, because we know from past experiences that you can go anywhere in the United States, any city, and you are probably going to find someone on a street corner or somewhere who is selling birth certificates, Social Security cards, documents that can be used to obtain a driver's license and apply for a U.S. passport ultimately. I do not think in my experience that these so-called document vendors selling these breeder documents would think twice about selling it to someone who was here to commit terrorism or bank robbery or anything else. They are out to make the quick buck.

These documents can sell for anywhere from $200 to as much as $6,000 for sometimes a very poor quality document. So I think it would be relatively easy, unfortunately, for someone with these ideas in mind to do this.

Chairman COLLINS. Mr. Ford, the GAO found that although the Terrorist Screening Center has been operational since December 2003, the State Department and the Center did not even begin exploring the possibility of linking the names in the Terrorist Screening Center system with the State Department's name check system for passports until December 2004, and it is my understanding that even today that link still has not been established.

In your judgment, why did not the Terrorist Screening Center start sharing information with the passport name check system at the same time that it started sharing information with the State Department's name check for visas?

It is odd to me because there is sharing of information on visas, but there appears not to be sharing of information on American citizens with ties to terrorism.

Mr. FORD. It is unclear to us why the information was not shared initially when they stood up in December 2003. We have been told that the focus initially was on the visa issue. We were concerned about foreign aliens, potentially bad people that live in other countries. The TSC visa system was set up so that they could reduce the vulnerability in the visa world. But it is not clear to us why passports were not thought of as another potential vulnerability for sharing that information.

So, again, we never really got a very clear explanation as to why the passport area was not considered at the time they set up the Terrorist Screening Center.

Chairman COLLINS. Mr. Johnson, do you have any insights on that? Did the State Department think about asking the Terrorist Screening Center for its complete watch list?

Mr. JOHNSON. No, ma'am. I have no knowledge as to why that was not done.

Chairman COLLINS. Mr. Ford, we find a similar problem dealing with criminal fugitives and the FBI not sharing the names of many State and Federal fugitives, including those, as your testimony pointed out, who are wanted for very serious violent crimes. Once again my question is the same. Why did not the FBI make certain that the State Department had access to its list of fugitives in order to prevent one of them from getting a passport and fleeing the country?

The regulations prohibit the issuance of a passport to someone with an outstanding Federal warrant. It seems a logical step to have been taken.

Mr. FORD. Well, again, I do not know completely the reasons why that information was not being shared. The State Department indicated to us early on in our assignment that they believed that they were getting Federal warrants through the U.S. Marshals Service, and as the course of our work went on, we found that, in fact, the U.S. Marshals Service database does not contain all Federal warrants and that the FBI is a better database, is more comprehensive, and includes not only Federal warrants but also State warrants.

So again, it is not clear to us why this issue was not pursued by the Department of State in terms of getting access to the information. We do know that there was a dialogue between the FBI and the State Department in late 2004 up through just recently, we understand, about trying to find a way to share this information.

It is not really clear to us why this was not considered early on as a way to again foreclose a vulnerability.

Chairman COLLINS. Mr. Johnson, the GAO, in its computer match, uncovered a case of a fugitive receiving a Federal passport, an American passport, even in just the limited review that it did. Have you had any experience with a fugitive trying to apply for a passport at the office for which you worked?

Mr. JOHNSON. Yes, ma'am. In late 2003 there was an individual who had committed a murder in Georgia, and it was about 2 or 3 days previously. I guess the police had received a tip that this individual was driving to Miami in an attempt to get a U.S. passport in his true identity to leave the country. So they just called our office. Basically the duty agent answered the phone, and it was about 1:30 in the afternoon. And the agent said, "Well, let me go check, take the name and go down to the passport agency and check and see if this person had applied." And in fact, when she went down, the person had applied for a U.S. passport and was coming to pick it up within the next hour, and the passport was going to be issued.

So what happened was when he came to pick it up, two of my agents detained him and his vehicle, which he had actually used in the commission of the crime, and we were able to turn him over to State authorities.

I would add that while he was not a Federal fugitive, he was a State fugitive, a very brutal murderer, who later was convicted and sentenced to life in prison.

Chairman COLLINS. But for that tip, the individual would have been able to pick up the passport and flee the country; is that correct?

Mr. JOHNSON. Yes, ma'am.

Chairman COLLINS. So it is not because there was an information sharing system in place that this was discovered. It was due to a tip which was followed up on quickly.

Mr. JOHNSON. Yes, ma'am.

Chairman COLLINS. Thank you.

Senator Carper, I know you are on a tight schedule. I have some additional questions for our witnesses, but I would like to yield to you.

Senator CARPER. Thank you, Madam Chairman. I was just handed a note that said my 10:15 call has been rescheduled for 3 o'clock.

Chairman COLLINS. In that case I will reclaim my time. No, go right ahead. [Laughter.]

Senator CARPER. Thanks, Madam Chairman.

And to our witnesses, thank you for joining us today. I do not care who responds to this question. Either of you are welcome to. But a person in this country who is interested in getting a passport fraudulently, how might they go about it?

Mr. JOHNSON. The first thing, as I said earlier, they would have to prove is their U.S. citizenship and their identity. Typically they would either steal or buy some type of birth certificate from a State. In some States, unfortunately, it is relatively easy to go in and just get a copy of a birth certificate without any proof of identification. So they would procure or obtain a birth certificate from some State or one of the territories.

Senator CARPER. Could you slow down just for a second? So a person alleging to be me or you or anybody else in this room might be able to go to an agency within their State and ask for a birth certificate, not have to present identification?

Mr. JOHNSON. In some cases that is correct, yes, sir.

Senator CARPER. And obtain that?

Mr. JOHNSON. Yes, sir.

Senator CARPER. Is that commonplace?

Mr. JOHNSON. It happens. I can think of numerous cases where that has happened. But if they do not do that, certainly, as I indicated earlier, there are plenty of people out there on the streets who are illegal document vendors, and you can buy blank birth certificates where you essentially fill in the blank, what name do you want to use. You can buy birth certificates that are legitimate in someone else's identity, and then they typically would take that birth certificate and apply for a driver's license or a State ID card. And with those two documents, that should be sufficient, that is all the information that is really needed to go and apply for a U.S. passport. It can be a relatively simple process.

Senator CARPER. Mr. Ford, would you concur with that?

Mr. FORD. Yes. In our discussions with the Diplomatic Security Service, the individuals who investigate these type of cases, use of eligibility documents like driver's license, birth certificates can be used as a vehicle to illegitimately get a passport.

Senator CARPER. My staff, as they sometimes do, gave me several questions that I might want to consider asking. The first question starts off and says, it seems to me like our first line of defense against passport fraud are the men and women who work at places

like the Postal Service that accept passport applications and forward them to the State Department for review.

In listening to this testimony today, Madam Chairman, I am reminded the first line of defense probably is not the Postal Service, it probably starts well before that in some of these agencies that you are talking about that can issue a driver's license or a birth certificate, or for the lack of enforcement to crack down on folks who might be out on the streets trying to sell these bogus documents.

How do we confront and deal with the sort of situations that you just described?

Mr. JOHNSON. One, I think this is a big step because I think it serves as a recognition that on Capitol Hill everybody is looking at this, is this a problem. I am of the mindset that we should always be proactive and not just react, and I think if you give, for instance, Diplomatic Security the adequate special agent resources to actively pursue these so-called document vendors, I think you start in a proactive manner, starting to eliminate and make it very difficult for these people on the street to vend these and sell these documents.

Another way, quite frankly, is the sentences handed down when you have someone convicted of passport fraud are very small typically.

Senator CARPER. Give us some idea what the range of sentences might be for a first offense and multiple offenses.

Mr. JOHNSON. Someone with no criminal history, never been convicted of a crime, they typically would get probation if convicted of passport fraud. I can remember cases where someone who has maybe been arrested multiple times on very heinous crimes but never convicted. Therefore, it does not kick it up in terms of the guidelines. So what would happen, that person would get essentially probation or certainly less than 6 months, and I think that is a huge problem in the system because it serves as no deterrence and it serves as no punishment. I think if we recognize that it is something that we want to go after, then we have to have a punishment that meets the crime. In my estimation it totally undermines a lot of our homeland security efforts by allowing these people to go out there and commit this crime.

Senator CARPER. In whose courts would crimes of this nature be tried, and in your own view—and this would be for either of you—what might be more appropriate sentences, particularly for multiple offenses?

Mr. JOHNSON. These are all going to be tried typically in Federal courts, U.S. Attorneys Offices around the country prosecuting these cases.

We did a big study a couple of years ago trying to promote the U.S. Sentencing Commission an initiative to raise the so-called guidelines, base offense levels for passport and visa fraud. We did a pretty in-depth study in terms of what would be appropriate, and essentially, we looked at some of the other like crimes, for instance, perjury before a government official or a grand jury, false statements to a Federal agent. Typically those crimes can get someone in the 18- to 24-month time frame. And we sort of made the connection that, OK, if you are fraudulently applying for a U.S. pass-

port you are essentially under mining homeland security. That we think would be appropriate range for someone who commits this crime.

Senator CARPER. Mr. Ford, any thoughts?

Mr. FORD. We really did not look at the sentencing issue per se. The few cases that we identified that we did some research on, we found that although the sentencing for passport fraud may not have been extensive in terms of amount of time, often they were connected to other much more violent crimes, so the individual, in a few cases that we looked at, would be prosecuted for the more violent crime. So the fact that they were apprehended allowed Federal or State authorities to prosecute them for more violent crimes, which of course had much longer potential sentences. But we have not studied this issue.

Senator CARPER. Share with us, if you would, the range of the kinds of people who might be seeking a passport fraudulently. The ones we might be most concerned about are those who may be terrorists or seek to commit some terrorist act. I am sure there are some that are more benign. But just give us the range of uses or backgrounds of the people that we are concerned about here.

Mr. JOHNSON. Certainly in the 5 years I was in Miami, the extremes were several murderers that were attempting to get U.S. passports and different identities. I can think of probably two or three cases right off the top of my head where someone wanted for murder in a State was attempting to get a passport in a totally different identity, bank robbers——

Senator CARPER. For the purpose of leaving?

Mr. JOHNSON. For the purpose of leaving or just melding into society. There was one case where it was an individual out of Maryland who had allegedly killed a person and seriously injured another. He came down to Florida, bought one of these rather cheap counterfeit Virgin Islands birth certificates.

Senator CARPER. What do they cost?

Mr. JOHNSON. I do not recall what these things range. One person paid $6,000 for one of these documents. I mean on face value you could tell it was not a very good document, but to the criminal, OK, it is $6,000, it must be worthwhile.

Senator CARPER. What do they go for up in, say, Bangor, Maine? [Laughter.]

Just kidding.

Mr. JOHNSON. I am thinking about the Miami market. So this individual came to South Florida, bought one of these counterfeit Virgin Islands birth certificates, had the name typed in using a totally different made-up name. And I had a really impressive agent who worked the case, realized right up front that it was a fraudulent case. He went and got an arrest warrant in that bogus identity because our efforts to find him were negative. So he put him in NCIC, and then a short while after that a police officer in Palm Beach County stopped this individual on the street corner, and the individual handed him his driver's license and this bogus identity, and the warrant came up wanted by Diplomatic Security for passport fraud. So we still did not know who this individual was.

We put him into our custody, fingerprinted him, and soon after the fingerprints came back from the FBI we realized who he was

because he was wanted for murder in Maryland. And that is a classic example of had it not been probably for an aggressive young Diplomatic Security agent, this murderer, who had a totally clean identity, and apart from having been fingerprinted and having his fingerprints in NCIC, he might still be walking free.

Senator CARPER. Madam Chairman, my time has expired. Could I ask one more question?

Chairman COLLINS. Certainly.

Senator CARPER. Thank you very much.

Talk to us about what other ways that we can, using technology that we have today, that we can better ensure that the person who is applying for a passport is indeed the person that they say they are.

Mr. JOHNSON. There are so many different governmental databases, law enforcement, intelligence, private sector, in my mind something as important as issuance of a passport, you should have as many cross-checks as possible. To me, having stovepipes of different systems where only certain agencies can get to it, or even stovepipes within your agency, totally defeats what we are trying to do here. To the extent possible, even if we have to pass laws to allow NCIC to be passed to Consular Affairs, then maybe that is what we need to do because I think we have to be extremely aggressive in developing systems, intelligence and law enforcement sharing to prevent these types of things. To me that is a big step.

Senator CARPER. Mr. Ford, would you answer the same question, please?

Mr. FORD. I totally concur that I think the issue of sharing appropriate information with all the various parties involved is critical to this process because the examiners in the passport area, if they do not get a hit that an individual is somebody they ought to be worrying about, then they are not going to know not to approve the documentation for the passport. I think this is the most critical issue.

I think with regard to at least the management of the process, and as we say in our report, there is a need for more training. Training was very inconsistent in the passport offices. The acceptance agents, we have 7,000 of those around the country. It is not clear to us to what extent individuals at post offices and county clerks, places like that, are well trained in this area. So I think our focus is on better training, better awareness of what some of the fraud indicators are, better information sharing, that those things in total should help prevent fraud more than it is currently based on our analysis.

Senator CARPER. The last thing, just as succinctly as you can, what should we do? Senator Collins, our Chairman, those of us who serve on this Committee, what should we do?

Mr. FORD. I think that the one issue, again, we have not studied it in detail, but I think there are some legal issues regarding what can be shared between the law enforcement community, basically the FBI and the State Department, that may require some legislative changes.

Senator CARPER. Mr. Johnson, what should we do?

Mr. JOHNSON. I would hope that as a result of these hearings, that the Department of State, both in Consular Affairs and in Dip-

lomatic Security, would come forward with some initiatives for additional resources. Throughout the report they cite resources as one of the problems, and quite frankly, I think that is something that this Committee maybe can help them resolve.

Senator CARPER. Our thanks to both of you. Thanks, Madam Chairman.

Chairman COLLINS. Thank you.

Mr. Johnson, I want to follow up on that last question. We have talked a lot about the vulnerability created by a lack of information sharing. You have been on the front lines. You have mentioned that the inadequate penalties are another issue that needs to be addressed, but what about staffing, training? Is there a sufficient staff that is dedicated to passport fraud? Talk to us more if you will about the personnel and resource constraints that the GAO identified.

Mr. JOHNSON. I will sort of split in both halves, first with Consular Affairs and their passport agencies. I was still at the Agency when they made the decision to eliminate their assistant fraud program managers. This was I think in early 2004. I recall at the time telling the various Consular Affairs officials that I really felt that was not a very good idea. Many of these assistants had been in those jobs for years and years, and had a great deal of local and national knowledge when it came to fraud. I recognize what the Department's idea was, to rotate the examiners through to get everybody a little bit of a sharing of how fraud works, but in my mind, why not leave the assistants there and then still rotate? You are in essence multiplying your ability to identify fraud.

I guess they had their reasons for doing it. To me, coming simplistically from a law enforcement standpoint, they literally are the ones who have to identify the fraud. Why would you want to shorten or potentially shorten or short staff yourself? I think that is one thing from a resource standpoint, that if anything, they should be beefing this up. I know that they are looking at a period where the issuance of passports—they are looking at maybe from 8 million to potentially 12 million. With that is going to come a lot more fraud. I think you should be beefing up your efforts as opposed to cutting back or shorting.

On the Diplomatic Security side, there is no organization that is better at doing what they do, but the problem is they have too many missions. The summer of 2004 in my field office at the time was approximately 50 special agents, and at any given time I would have five or six of my agents on rotation to Baghdad to the temporary duty assignments in Iraq, not to mention Kabul, Afghanistan, and other protective security details. So it was literally moving chess pieces. Who am I going to have this week? Because those agents were being pulled for other priority missions.

I think there has to be a recognition that this is a problem and that they have to dedicate the number of resources they need to combat this problem, and that is simply what it comes down to. I think they have the expertise, but they need the intelligence, as I mentioned in my statement, they need intelligence ability, and they just quite simply need more agents.

Chairman COLLINS. Mr. Ford, I could see you nodding your head in agreement when Mr. Johnson was outlining the personnel and

resource challenges. What did the GAO find with regard to adequate staffing and also the elimination of the assistant fraud manager position?

Mr. FORD. We visited 7 of the 16 passport offices, and we telephonically contacted the fraud prevention managers in all the other offices. A fairly consistent message we heard was that the elimination of the assistant fraud prevention manager was viewed as hurting the effort to look at fraud.

The Department wanted to expand training by having individuals put in a rotational program. That made sense to us, but the elimination of the assistant position, given the workload problems that the fraud managers had in most of the posts we visited, did not seem like was a good idea to us. Our recommendation, basically we went to the State Department and said, we think you need to reexamine the overall staffing profile here because, again, the message was fairly consistent in almost every passport office we visited. They said that this is hurting the effort to identify potential fraud.

As Mr. Johnson indicated, if the volume of passports is going to continue to grow over the next several years, it seems the problem will be compounded unless there is enough people out there who are trained in fraud prevention to really put a kink into the potential that could be out there of the country being vulnerable.

Chairman COLLINS. Mr. Johnson, in your testimony you describe fraud rings that sell bogus breeder documents such as birth certificates that are in turn used to secure a passport. What is your evaluation of Federal efforts to crack down on these fraud rings? Is there an organized Federal effort to go after these rings that are selling the breeder documents?

Mr. JOHNSON. Not that I am aware of. I think it really always came to—and I have worked all over the country in the passport fraud arena—and it always came down to regional nuances. I mean in some regions you might have—Diplomatic Security would be aggressive in pursuing these document vendors, and maybe the former Immigration, now Homeland Security, ICE, would be aggressive. Other areas, the FBI might have an interest, but unfortunately, I cannot say across the board that any particular agency or any group of agencies would wholeheartedly go after these rings. In my mind, again, I think that is a little bit of a lapse, that we need to sort of have a consolidated across the U.S. approach to combating this problem.

Chairman COLLINS. That does seem to be an important gap because if you can break the rings that are providing the bogus documents, you prevent the person from getting the passport in the first place.

Mr. JOHNSON. If I might add, sometimes—and I think the report refers to this—that most of these individuals were not successful in getting these passports issued, but you still have an individual with a new birth certificate and a new identity. While he or she may not have gotten the passport, they are still out there walking around with a driver's license and a birth certificate and a different identity. What are they doing? It is just something that maybe the State Department will—I am just saying that is a whole——

Chairman COLLINS. A whole other area for us to crack down on. Thank you.

Mr. Ford, just one final question. On its comments on the GAO's report, the State Department points to a new series of unannounced audits that it is conducting that it started in April to determine the effectiveness of anti-fraud programs at various passport offices. And the State Department officials have trumpeted these results in saying that they show only very minor errors. What is your response to that?

Mr. FORD. First of all, we have not examined their audits in detail. We have seen some information regarding the reported results. With regard to the issue that it appears to be a minor problem, looking at their analysis, I believe they extrapolated their sample by indicating there could be the potential for 4,000 cases, if they extrapolated to all the passports being issued. If that were the case, since I believe they referred around 3,200 cases last year, that would indicate that the potential for fraud is a lot greater than what was reported last year through their fraud prevention system.

So again, I have not examined it in detail. I think it is good that they are doing it, but it does point to the fact that the potential for more fraud out there may be greater than what they suggest.

Chairman COLLINS. Thank you very much for your testimony. Senator Carper.

Senator CARPER. I have no further questions. Again, our thanks to both of you. Thanks, Madam Chairman.

Chairman COLLINS. Thank you very much. Your testimony has been extremely helpful, and we look forward to working further with you.

Mr. FORD. Thank you.

Mr. JOHNSON. Thank you.

Chairman COLLINS. I would now like to call forward our second panel, which brings together three accomplished Federal officials with the responsibility for issues related to the security of the U.S. passport system.

Frank Moss is the Deputy Assistant Secretary of State for Passport Services. He is responsible for overseeing the processing of some 8.8 million passport applications last fiscal year.

Donna Bucella is the Director of the Terrorist Screening Center and is on detail to the FBI from the Transportation Security Administration, where she was the Southeast Area Director.

Thomas Bush began his FBI career in 1975 in the Identification Division. Last December he was appointed by Director Mueller to be the Assistant Director of that division, now called the Criminal Justice Information Services.

I want to thank all of you for being here today, and we will start the panel by hearing Mr. Moss's testimony.

TESTIMONY OF FRANK E. MOSS,[1] DEPUTY ASSISTANT SECRETARY FOR PASSPORT SERVICES, BUREAU OF CONSULAR AFFAIRS, U.S. DEPARTMENT OF STATE

Mr. MOSS. Good morning, Madam Chairman and Members of the Committee.

I am pleased to be here today to discuss how the State Department is responding to concerns raised by the Government Accountability Office in its report, "Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts." I want to thank the GAO and especially their lead examiner, Michael Courts, for their hard work on this project. As the GAO report recognizes, the Department of State, especially the Bureau of Consular Affairs and the Diplomatic Security Service, are working hand in hand with elements of the Homeland Security and Justice Departments to protect the integrity of the U.S. passport. We acknowledge, however, that it is always possible to improve, and welcome GAO's observations and suggestions.

The integrity of the passport rests upon three major elements, the quality of the adjudication process, the security features of the passport itself, and the introduction of biometrics to make certain that the passport can only be used by the person to whom it is issued. This is what I illustrate on this charts to my right.[2] Taken together these elements form a comprehensive approach to passport security. Securing the document and the adjudication process is particularly important in an era when terrorists, transnational criminals, and others seeking to enter the U.S. illegally, view travel documents as valuable tools.

While my written statement discusses this in greater detail, let me highlight for the Committee just a few steps we are taking to improve the passport's design and to introduce biometrics.

We recently completed the first cover-to-cover redesign of the passport in more than a decade. The new document will include a host of new security features. These include sophisticated new art work, printing techniques used in the current generation of U.S. currency, and other changes that will significantly increase the physical security aspects of the U.S. passport.

This next generation U.S. passport, the e-passport, also includes biometric technology that will further support the government's border security goals. The e-passport includes a contactless chip in the rear cover that will contain only the data on the biographic data page of the passport and a digital image of the bearer. I am happy to share examples with the Committee, and some of the art work here to my left demonstrates the new security features and some of the other aspects of the new passports.

Let me discuss the GAO's recommendations and how the Department of State is implementing them. We agree with the GAO that enhanced interagency data sharing can significantly improve passport adjudication. We have taken numerous steps to meet that objective. For example, in April 2004 we signed an MOU with the Social Security Administration that allows us to verify Social Security numbers of U.S. passport applicants. We have a longstanding and

[1] The prepared statement of Mr. Moss with attachments appears in the Appendix on page 54.
[2] The charts referred to appear in the Appendix on pages 63–65.

effective working relationship with Federal law enforcement agencies. Today we have nearly 50,000 names of fugitives or other persons of interest to law enforcement in the passport lookout system. Half of those entries were made individually as a result of our outreach efforts. The other half are based on data transfer from the U.S. Marshals Service on persons subject to Federal fugitive warrants.

To complement this information, we are working with the FBI to add to the passport lookout system an extract of information from their NCIC database. I am happy to report that last week I received a letter from Mr. Bush that responds positively to our request for access to this information. We appreciate this positive response which we believe will enable us to include in the passport lookout system information on persons subject to State or local warrants. This is a long-sought objective of ours.

We have also just signed an agreement with the Terrorist Screening Center that will provide us information on American citizens who may have a nexus to terrorism or to an ongoing investigation. Under this agreement the State Department will inform the TSC whenever any such individual applies for passport services. In addition, the Department of State provides the National Counter Terrorism Center, NCTC, access to our PRISM database which includes images of all passport applications since 1994 including the photographs of the applicants.

GAO also recommends creating a national fraud library of suspect documents. There are several different resources containing such information, and we agree that finding a way to bring them together is desirable. In this regard we are pursuing access to the U.S. Secret Service's Questionable ID Documents (QID) database. This database includes sections on valid documents, stolen documents, and on counterfeits and alterations. A significant advantage to this initiative is that we at the State Department can contribute to the Secret Service's database, and therefore assist them in their mission, and of course it will also allow us to avoid significant development costs because we will piggyback on what the Secret Service is already doing.

The GAO recommends designating additional positions for fraud prevention coordination and training in domestic passport agencies and establishing a more formalized fraud prevention training program. We agree and have taken several steps to make this happen. We are adding more fraud prevention managers to the staffs of our larger passport agencies. We have increased the number of persons working in the fraud offices as well as the length of time they spend there. These are on rotational assignments. This will have a direct, positive impact on improving training provided to the passport specialists who adjudicate passport applications and stand as the first line of defense against passport fraud.

Finally, under a Washington-based reorganization, we will add to the staff that coordinates and backstops fraud prevention operations. Part of the work of that expanded staff will be to develop a national fraud training program for passport specialists.

The GAO also looked at workload transfers from one domestic passport agency to another. We do this, quite honestly, to make the best use of our issuance capabilities nationwide. A theoretical risk

in doing so is that we could miss opportunities to identify fraud. We believe that we address this risk successfully through our selection of highly skilled fraud program managers, by rotating senior passport specialists through the Fraud Program Management Office, so that they can assist and better train their staff, and by training all of our newly hired specialists centrally.

Finally, the GAO suggested increased training and oversight of the more than 7,000 passport acceptance agents nationwide. These are, as you noted in the earlier round of testimony, principally U.S. Postal Service employees and clerks of court who accept applications from U.S. citizens and identify the passport applicant as the person he or she claims to be. This is, of course, only the first step in the passport adjudication process.

Improved training is already under way through use of Computer Based Training modules developed in cooperation with the U.S. Postal Service that we are also adopting for use by other facilities and deliverers of acceptance agent services.

We are also exploring initiatives to better monitor the quality of the acceptance agents' work.

Chairman Collins, other Members of the Committee, thank you, and at this time I am happy to answer any questions you may have.

Chairman COLLINS. Thank you very much. Ms. Bucella.

TESTIMONY OF DONNA A. BUCELLA,[1] DIRECTOR, TERRORIST SCREENING CENTER

Ms. BUCELLA. Good morning, Chairman Collins. Thank you for the opportunity to discuss the missions and objectives of the Terrorist Screening Center as they relate to information sharing with the Department of State.

The mission of the Terrorist Screening Center is to consolidate the government's approach to screening terrorism and to consolidate the identities of all known and suspected terrorists into a single database.

The Terrorist Screening Center represents one of the most unique support organizations to terrorist screening and law enforcement operations ever conceived or implemented. The TSC has been providing key resources since December 1, 2003, including a single coordination point for terrorist screening data, the Terrorist Screening Center's database, a 24/7 call center for encounter identification assistance, access to coordinated law enforcement response, a formal process for tracking encounters, encounter feedback to appropriate entities, and a process to address misidentification issues.

Since the TSC was established, the Department of State has been a significant contributor to all of our overall success. The Department of State is a full partner at the TSC, and one of my executive deputies is a Department of State detailee. The close on-site partnership with the Department of State has enhanced our ability to administer the Visa Security Advisory Opinion Review, the Visa Revocation Review, and nominations to our database. Additionally, the Terrorist Screening Center and State are working to ensure that appropriate officials will be notified when a U.S. person is list-

[1] The prepared statement of Ms. Bucella appears in the Appendix on page 66.

ed in the TSDB and/or applies for a new, renewed, or amended U.S. passport. And we have signed that agreement.

Visa Security Advisory Opinions are generated by the Department of State Consular Affairs officers when a visa applicant is, in fact, a possible match to the CLASS system. The Department of State personnel at the Terrorist Screening Center have reviewed over 138 Security Advisory Opinions since December 1, 2003, our inception.

Visa Revocation Reviews are conducted for new entries into our database to determine if those new entries have been issued visas before the derogatory information surfaced. The Terrorist Screening Center has reviewed over 52,000 new names to our Terrorist Screening Center database, and we have alerted the Department of State to about 850 cases of possible visa revocation.

The Department of State specialists assigned to the Terrorist Screening Center play a very important role in the Terrorist Screening Center nominations process. The specialists have the expertise to ensure that foreign individuals nominated for inclusion into the Terrorist Screening Center database are thoroughly evaluated and made available to overseas posts.

The screening of U.S. passport applications, a highlight of the May 2005 GAO report, is a collaborative initiative that began this past January when it was identified as a vulnerability and basically a screening opportunity, and proposed by our State Department representative that we get the names of U.S. persons listed in the TSDB and make them available to the Department of State during the passport application process.

As I mentioned, the Memorandum of Understanding (MOU) has been signed. The TSC looks forward to continued collaboration with the Department of State on this project. Since Homeland Security Presidential Directive 6 was issued on September 16, 2003, the Terrorist Screening Center and the Department of State have been partnering to protect our Nation's security through the robust sharing of terrorist information. The Terrorist Screening Center has provided support to those functions identified by the Department of State as priorities and will continue to expand our relationship. This close and continuing cooperation contributed to worldwide efforts to keep terrorists out of the United States and locate those who may already be in our Nation.

The Terrorist Screening Center thanks the Committee for the opportunity to provide clarity and looks forward to continued work with the Committee in TSC's efforts to consolidate the government's approach to terrorist screening.

Thank you.

Chairman COLLINS. Thank you. Mr. Bush.

TESTIMONY OF THOMAS E. BUSH, III,[1] ASSISTANT DIRECTOR, CRIMINAL JUSTICE INFORMATION SERVICES DIVISION, FEDERAL BUREAU OF INVESTIGATION.

Mr. BUSH. Good morning, Madam Chairman, and Members of the Committee, and our condolences to Senator Lieberman and his family.

[1] The prepared statement of Mr. Bush appears in the Appendix on page 69.

As you mentioned, I am the Assistant Director of the FBI's Criminal Justice Information Services Division, otherwise known as CJIS. By way of background, CJIS is responsible for five services to law enforcement: Fingerprint identification; uniform crime reporting; National Crime Information Center, also known as NCIC; the National Instant Criminal Background Check System; and Law Enforcement Online.

NCIC, the service which is of interest to this Committee today, is a computerized database of documented criminal justice information available to virtually every law enforcement agency nationwide, 24 hours a day, 365 days a year. Since its inception, NCIC has been a highly effective tool for information sharing with local, State, tribal, and Federal entities. NCIC is operated under a shared management concept between our State and local and Federal criminal justice users. The database currently consists of 18 files, 7 property files, and 11 person files to include the Wanted Person Files.

During NCIC's first year of operation, which was 1967, 2 million transactions were processed. In May of this year, NCIC processed an average of 4.6 million transactions per day, with an average response time of less than 0.06 seconds. On May 27 of this year, NCIC processed a record 5.2 million transactions in a 24-hour period.

I would like to outline some of NCIC files and features that assist in immigration and border security. The Foreign Fugitive File, established July 1, 1987, contains information on persons wanted in connection with offenses committed outside the United States. There are two types of records in the Foreign Fugitive File—Canadian records and INTERPOL records.

The Immigration Violator File was established on August 25, 2003. In 1996, NCIC implemented the Deported Felon File. Today, this is now a category of records within the Immigration Violator File. Immigration Violator File includes two additional categories of records, individuals wanted as absconders, and individuals in violation of the National Security Entry/Exit Registration System or NSEERS. As of July 1 of this year, there were 163,000 plus records in the NCIC Immigration Violator File.

The Violent Gang and Terrorist Organization File, or VGTOF, was implemented in December 1994. This file was designed to provide identifying information about violent criminal gang and terrorist organization members to protect the law enforcement community and the public. Traditionally, NCIC Person Files serve the needs of the criminal justice community and are supported by the judicial process. Most typically, a warrant is on file. However, with the creation of VGTOF, that philosophy was expanded to support law enforcement, investigative and information needs related to terrorism. When the Terrorist Screening Center became operation in December 2003, the FBI CJIS Division modified the NCIC VGTOF file to support TSC's mission.

VGTOF is the means to make the terrorist screening information available to the law enforcement community nationwide. When an officer hits on a VGTOF terrorist record, he is instructed to contact TSC for additional information on the subject.

The Department of State Bureau of Diplomatic Security is a fully authorized NCIC user when conducting criminal investigations. Additionally, the FBI has provided the Department of State Bureau of Consular Affairs with extracts of the NCIC Wanted Person, Immigration Violator, Foreign Fugitive files, VGTOF, and the Interstate Identification Index on a daily and weekly basis for inclusion in its Consular Lookout and Support System, as required by Section 403 of the U.S. PATRIOT Act. The Department of State uses the information to ascertain whether visa applicants have records indexed in NCIC which might preclude the issuance of a visa.

In April 2005, CJIS received a request from Department of State Passport Services for an extract of the FBI fugitives contained in the NCIC system. Our immediate response was that the FBI fugitives in NCIC, which is approximately 7,000, represent only a fraction of the more than one million felony and serious misdemeanor wanted person records entered into NCIC. We requested that DOS Passport Services work with us toward the ultimate goal of system interoperability and direct NCIC access for passport screening. As an interim step toward this goal, we have agreed to and have provided the requested extracts to them as recently as, I believe, Monday of this week.

In closing, I would like to thank you for allowing me the opportunity to explain the use of NCIC for immigration and border security. I would now answer any questions you might have.

Chairman COLLINS. Thank you, Mr. Bush. It looks like there has been some considerable progress made in the past few days.

Let me start, Mr. Moss, with a threshold question for you. Do you believe that terrorists are trying to get their hands on U.S. passports? Is this a problem?

Mr. MOSS. Madam Chairman, I am unaware of any reports of terrorists themselves, people we knew were involved in terrorism, attempting to get a U.S. passport.

Taking it a little bit more broadly though, obviously we are concerned about anyone who may be seeking a passport in order to flee prosecution or to engage in activities inimicable to our interests. That is why we think that these recent breakthroughs we have had on terrorists, on exchanging screening information with TSC and with the FBI, are major steps forward toward making our borders more secure and obviously making our passport screening system more robust than has heretofore been the case.

Chairman COLLINS. Let me read from testimony that you gave on the House side just recently. You said, "We at the Department of State are certainly aware of how sought after this document is, not only by American citizens with legitimate travel plans, but by illegal immigrants, as well as terrorists and others who would do this Nation harm. A key objective of the Department is to ensure that U.S. passports are issued only to persons who are legitimately entitled to them. This is particularly important in an era when terrorists, transnational criminals, and others seeking to enter the U.S. illegally view travel documents as valuable tools." This morning you seem to be giving a different answer.

Mr. MOSS. I am sorry, Madam Chairman, I misinterpreted your question. In my testimony earlier, and even in some of the comments I made today, I would like to differentiate between what

happens in terms of people applying for passports domestically, and then the misuse of lost or stolen U.S. passports around the world.

In the case of applying for passports in the United States, I am unaware of any information on terrorists doing so, but obviously, having the access to the TSC data will help us ensure that does not happen.

The other side of the coin is when passports are lost or stolen abroad. There is an active international market that supports illegal immigration, transnational crime, and yes, terrorism, trying to acquire lost or stolen documents, not just from the United States but issued by legitimate governments around the world. The 9/11 Commission dealt with this in depth both in its comprehensive report as well as in an appendix it wrote on the issue of terrorist travel.

In terms of trying to prevent the misuse of U.S. passports, I would mention, for example, that whenever we become aware of a lost or stolen U.S. passport, we provide that data to INTERPOL so that it can be shared with governments throughout the world. We have given INTERPOL information on some 660,000 lost or stolen passports over the last year. That is several years worth of data, but it shows our commitment to try to prevent the misuse of the U.S. passport.

We also invalidate the use of a U.S. passport for travel once it has been reported as lost or stolen.

And the third point I would say is we have taken dramatic steps to improve the physical security of the U.S. passport, so that one of the longstanding vulnerabilities, which was changing the photograph, the tactic we all saw in the movies made in the 1960's, that just simply cannot be done now. We think we have a very robust passport physically as well as systems to prevent the misuse.

Thank you.

Chairman COLLINS. Mr. Moss, I agree with you that the passport has improved greatly as far as becoming very difficult to counterfeit, but that is not the focus of the GAO report, nor our previous witnesses. What they are trying to alert you to are very serious vulnerabilities where phony breeder documents such as phony birth certificates or driver's licenses could be used to secure a legitimate U.S. passport. We are not talking about a stolen or lost passport falling into terrorist hands. We are talking about vulnerabilities in the system that could be exploited by terrorists using phony birth certificates to obtain a U.S. passport, and that is what the GAO has tried to alert you to, and that is what Mr. Johnson's testimony suggests is a real problem.

Mr. MOSS. Well, Madam Chairman, first of all, I do want to thank the GAO for their work. They have alerted us to areas we have to make improvements in. And I would like to thank you as well, because in the Intelligence Reform Bill that you passed last December, there were some important developments that apply to this very issue you have talked about, moves toward Federal standards for birth certificates, for example.

My understanding is that right now there are 8,000 different jurisdictions in the United States that issue birth certificates, and there are something like 50,000 different types of birth certificates

in circulation. The same applies clearly to the issue of driver's licenses.

The third point I would make is that is why it is so important, we believe, to give so much training and so much close management supervision to our passport specialists. These are the people we depend upon to identify fraudulent documents by their look, by their feel, by relationships between that document and what the passport application says. This is an area where we are making major investments.

The fourth point I would say is clearly we continue to strengthen our fraud prevention program activities. For example, mention was made of lost and stolen birth certificates issued here in the United States. We have a particular concern over one jurisdiction in the United States. We talked a little bit about Hudson County in the earlier round of testimony, but the other thing is that in one case involving, quite honestly, Puerto Rico, we do subject any passport applications supported by a Puerto Rican birth certificate to extraordinary security reviews before issuance because of our concern over the security of that document.

So we do have, I believe, a robust system in hand, and it will only get better as we move toward Federal standards on driver's licenses and birth certificates.

Chairman COLLINS. If you are not currently receiving information from the Terrorist Screening Center on Americans who are on the watch list, how would you know whether or not an American with ties to terrorist groups is receiving a passport?

Mr. MOSS. The way I would answer that is the following. For about a generation we have depended upon a push system in which Federal agencies and State and local law enforcement authorities have shared data with us on persons of particular concern to us. We are now trying to go to a system where basically we pull that data from other databases. That is why access to the TSC database is so important. The same applies to Mr. Bush's offer of access to NCIC. I think we have a good system right now. Can it get better? Yes. And I think that the GAO report has advanced that process. The cooperation of my colleagues here at the table will help us to do a better job in the future.

But let me assure you, if any agency at this table or another Federal agency or a State or local authority has a concern about an individual, they can tell us right now. They know how to get in touch with us. We will put that person in the lookout system and prevent passport issuance to them until we have resolved that problem.

Chairman COLLINS. Mr. Moss, in your written testimony you said the Department of State is about to sign an agreement with the Terrorist Screening Center that will provide information on American citizens who are of concern to TSC due to the nexus to terrorism or an ongoing investigation. I believe I heard you say this morning that you have signed it. Could I ask when it was signed?

Mr. MOSS. It was signed last evening by the two agencies, including by Donna Bucella here at the my left.

Chairman COLLINS. See, sometimes oversight hearings do have the desired result. [Laughter.]

I am very pleased to learn that it has been signed. I think that is a really important improvement to make.

Ms. Bucella, let me ask you, the Terrorist Screening Center was sharing information on visas with the State Department, why was there not sharing of information on U.S. citizens of particular concern?

Ms. BUCELLA. Chairman Collins, I wish that I could tell you when we set up the Terrorist Screening Center I just went around to different government agencies and knocked on their doors and they gave me their list.

What we have had has been a tremendous effort in trying to gather the names of all suspected, known, international and domestic terrorists from all the different agencies. What we had to do is gather information in various forms. Some had full names, some had partial dates of birth. We had to prioritize, and still trying to gather our arms as the U.S. Government as to all the names.

And so one of our first priorities was preventing people from coming into the country, and so we went through the—obviously, when we were set up, the State Department donated part of their Tipoff staff to us, but that Tipoff staff dealt solely with those individuals that were applying for visas, keeping people outside the country. So we loaded up our system using the Tipoff system. It was not until, I believe, January of this year, when we were having discussions with the State Department, that we realized that there was yet another screening opportunity, and that was the U.S. passports.

And so the reason why—I read the GAO report, and when it had that we were not cooperating, we were. We were just trying to figure out what it is that you want, what it is that you need, and how can we get it to you. And so that was the discussion that we have had over the last couple of months with our lawyers and making sure that we complied with the privacy laws and things, and that is why we have recently just signed the Memorandum of Understanding.

The implementation of this—because it is a technology issue, it is really the connectivity—will be done before August of this year.

Chairman COLLINS. Mr. Moss, did the State Department ask for this information?

Mr. MOSS. Madam Chairman, we have an effort going back 2 or 3 years now, trying to reach out to Federal agencies to acquire additional information to put into our screening system. One of our first successes was the U.S. Marshals Service. We were then looking for other databases. By last December the letter left us and arrived in January at TSC, it is almost immaterial. Between ourselves we identified an opportunity to strengthen our passport lookout system by incorporating the TSC's information, and we have been working together since then.

And I would say the same applies to the FBI. We are trying to make this database richer, and now of course, not only do we have an offer of 7,000 additional names of persons subject to Federal warrants, but this great development over access to persons who are subject to State warrants and local warrants as well.

Chairman COLLINS. Mr. Bush, that leads me into a question for you. It seems to me that the FBI has a very strong interest in mak-

ing sure that fugitives do not gain access to passports that they could use to flee the country. Can you explain to us why the FBI took so long to make the names of its fugitives available to the State Department so that you could be alerted if one of these fugitives applied for a passport? I find it so inconceivable that we have posters of the Ten Most Wanted in our Post Offices, and yet we are not sharing that information in databases throughout our government.

Mr. BUSH. And let me backup what Mr. Moss has said. Historically—and I was a fugitive hunter in the 1980's in the Washington Field Office, and we were always encouraged and had procedures to put stops individually, as he says, in a push type of format with the State Department, and we often did individually. So case agents—and I cannot speak about these particular cases that were up here—had the opportunity, always have had, and I know we took collectively large numbers of fugitives and persons of interest and put them in the Tipoff system, which when CLASS was searched would designate the fact that they were wanted. But clearly, with the examples given here, there were opportunities to catch individuals that were applying that were not taken advantage of by our case agents on an individual basis.

So as we move into this process to ensure in their pool process to get as many in there as we can, then we will clearly fill some of those gaps that we have had. But it has always been—I remember doing it myself with the State Department, so always had that option. We clearly did not put all of them in there.

I think some of it was a resource issue. When you talk about issuing 10 million passports a year that are name-based, when NCIC records about a 10 percent or plus 10 percent hit rate, so you are looking at about a million hits there on names that are phonetic searches. And they did not even used to be exact date of birth, they had a range. So you would pull out a lot of false positives. So you had an impact there on resources at the State Department and within the FBI, and that is what we need to work around with access even to these 1.2 million fugitives. That is going to create a lot of hit activity. That is the back side to sharing information. It is the what do you do with it when you get it and you get these hits? That is what we want to work with them closely with, to a mutually agreeable system of applying that service.

Chairman COLLINS. It seems a very burdensome, labor-intensive process, however, to rely on individual case agents trying to guess whether a fugitive is at risk of flight and alerting the State Department. It seems much more efficient to have a database sharing where perhaps you do not share all 1 million fugitives' names, but you do those convicted of serious crimes. I mean it seems to me that you can deal with the data issue overwhelming the system by selecting it based on the seriousness of the crime, but it is disturbing to me that the GAO's limited review found so many instances of fugitives who had committed extremely serious crimes, and yet were not included in the State Department system, and indeed, the GAO, despite a very limited review, was able to come up with some very egregious cases.

So I hope the FBI will work to come up with a system that automatically shares the names of fugitives who have been convicted, or who are wanted for serious crimes.

Mr. BUSH. And clearly, there are more effective means. There are other means with checking passenger manifests and putting stops in the Treasury enforcement computer system that would also pick up on some of these fugitives' travel, and the fact that they obviously do not always use their true name. In the case here, they obviously did.

But I think our mutual goal is to do the best we can and to make it better wherever we can, whether it is terrorist related or fugitive related.

Chairman COLLINS. Mr. Moss, one other question for you. We talked a lot about the information sharing challenges and the need to improve that, and indeed the agreement signed last night, I think, is a very good step in the right direction, as well as good timing for this hearing.

But the GAO and Mr. Johnson also identified a number of other weaknesses in the State Department's overall fraud prevention program. For example, GAO was critical of the limited oversight and training of acceptance agents, the lack of a consistent nationwide training program, the absence of a centralized and up-to-date electronic fraud prevention library, and the fact that headquarters' responsibility for fraud prevention support is somewhat unclear. Mr. Johnson raised concerns about the elimination of the assistant fraud manager position, and suggested also that not enough resources are focused on fraud detection and prevention.

What steps is the State Department taking to address these concerns which are organizational, resource, training, or oversight concerns?

Mr. MOSS. I think we are in fact addressing each and every one. Let me begin with the issue of the so-called elimination of the anti-fraud, assistant anti-fraud program managers.

What we had was a situation where we had a couple of people encumbering these positions and some other people who had been assigned to this function basically on informal details at the passport agency level. What we are trying to do, Madam Chairman, in this effort, is to make certain that the knowledge that is held by our fraud program managers really gets to—for want of a better term, the passport floor. Passport fraud is identified by our passport specialists. They are the people who literally see the application, look at databases, touch the birth certificates and things like this.

What we are trying to do by our current strategy is to rotate our supervisory passport specialists through the anti-fraud program office, have them spend 3 to 6 months there, understand the anti-fraud tools, and then go back to help train their own staff.

Second, we have also implemented a centralized training program for our new passport specialists so that they all have a thorough grounding in passport fraud detection efforts.

I should also talk a little bit about resources, both in terms of the passport side, and I would also like to mention briefly some developments on the Diplomatic Security side. We are continuing to hire additional personnel. Our workload is growing dramatically.

You are well aware, of course, of the Western Hemisphere Initiative that is coming along as well. We are not trying to overburden our staffs. We are trying to hire and keep our staff ratios in line with our workload. Also our colleagues at Diplomatic Security have gone to a new model for staffing their own offices around the country. They are beginning to assign civil service personnel to those offices as investigators so that they have the long-term continuity that Mr. Johnson mentioned in his testimony.

On the question of the acceptance agents, I think there are two things I would like to mention. First of all, most of the acceptance agents are employees of the U.S. Postal Service, have been vetted by the U.S. Postal Service, and are U.S. citizens. The U.S. Postal Service has developed a computerized-based training program for those people. We are so impressed with it that we are actually acquiring rights to use it to help train those non-Postal Service acceptance agents, clerks of court, a handful of universities, things like this, some public libraries around the United States. We also use our own customer service staffs in the passport agencies to do outreach to these agencies.

The final point I would say is that if an acceptance agent has any question about a passport application, they simply accept it, they flag it for us, and we take it from there. They have a very limited role, basically, to ensure that the person applying for a passport is who they claim to be. We make the decision on passport issuance. That is inherently a Federal Government responsibility.

So I really think that between our work with DS, the additional personnel we are assigning to the anti-fraud program responsibilities at our largest agencies, our rotational activities, and our training opportunities for all of our staffs that we already had in place, we have a robust strategy to help address many of the suggestions and recommendations made by the GAO.

Chairman COLLINS. Thank you for that summary statement.

I want to thank all of the witnesses who have participated in our hearing today.

As Mr. Moss indicated, this Committee spent a great deal of time last year drafting intelligence reform legislation—sweeping reforms. One of the major issues that we focused on in the hearings as a result of the 9/11 Commission report was the lack of information sharing among Federal agencies, a lack that prevented agencies from putting together the pieces of the puzzle that might have allowed us to thwart the attacks on our country on September 11, and that is why it is particularly frustrating to me personally to see that there are still serious examples of a lack of consistent information sharing that could be harmful to our homeland security.

In the case that the GAO has identified and that you are all working to remedy, it is particularly frustrating to me because it does not require a new law to be passed. It does not require a new Executive Order. It does not require a massive new appropriation. What it requires is simply to have agencies working together to share vital information to help protect our Nation against terrorists and other criminals who would do us harm.

I want to close this hearing by urging you to work very closely together to improve the system. I realize there are technological challenges. I realize there are the problems of false positives. But

in this age of databases and computers, surely we ought to be able to come up with a system that allows us to stop issuing passports to fugitives wanted for serious crimes, and to terrorists. I do not feel confident that we have such a system now. I believe we are making progress, and I think the agreement signed is a major step in the right direction. But I urge you to redouble your efforts. This is so important. I think Secretary Powell was correct when he said that the integrity of the U.S. passport is absolutely essential in the global war on terrorism.

So this is an issue that the Committee is going to continue to follow very closely. We look forward to getting an update from you as implementation goes forward, as you meet the August goal that you have set for implementation. I realize there will be challenges, both from technology and privacy concerns and other issues, but surely we can do better.

Again, I thank you for your cooperation with this investigation, and I look forward to working not only with this panel, but our previous one, to make sure that the system for issuing passports is as secure as it can possibly be. Thank you for being here today.

The hearing record will remain open for 15 additional days.

I want to thank the GAO for its excellent investigation in this area, and I want to thank my staff for their hard work.

This hearing is now adjourned.

[Whereupon, at 11:16 a.m., the Committee was adjourned.]

APPENDIX

United States Government Accountability Office

GAO

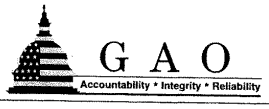
Testimony
Before the Senate Committee on
Homeland Security and Governmental
Affairs

For Release on Delivery
Expected at 9:30 a.m. EDT
Wednesday, June 29, 2005

STATE DEPARTMENT

Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts

Statement of Jess T. Ford, Director
International Affairs and Trade



GAO-05-853T

May 2005

GAO
Accountability · Integrity · Reliability
Highlights

Highlights of GAO-05-477, a report to the Committee on Homeland Security and Governmental Affairs, U.S. Senate

STATE DEPARTMENT

Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts

Why GAO Did This Study

Maintaining the integrity of the U.S. passport is essential to the State Department's efforts to protect U.S. citizens from terrorists, criminals, and others. State issued about 8.8 million passports in fiscal year 2004. During the same year, State's Bureau of Diplomatic Security arrested about 500 individuals for passport fraud, and about 300 persons were convicted. Passport fraud is often intended to facilitate other crimes, including illegal immigration, drug trafficking, and alien smuggling. GAO examined (1) how passport fraud is committed, (2) what key fraud detection challenges State faces, and (3) what effect new passport examiner performance standards could have on fraud detection.

What GAO Recommends

This report makes six recommendations to the Secretary of State to consider ways to improve interagency information sharing, establish a centralized and up-to-date fraud prevention library, consider augmenting fraud prevention staffing, assess the extent to which interoffice workload transfers may hinder fraud prevention, and strengthen fraud prevention training and oversight. State generally concurred with our recommendations and indicated that it has begun taking steps to implement most of them.

www.gao.gov/cgi-bin/getrpt?GAO-05-477.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Jess T. Ford at (202) 512-4128 or fordj@gao.gov.

What GAO Found

Using the stolen identities of U.S. citizens is the primary method of those fraudulently applying for U.S. passports. False claims of lost, stolen, or damaged passports and child substitution are among the other tactics used. Fraudulently obtained passports can help criminals conceal their activities and travel with less scrutiny. Concerns exist that they could also be used to help facilitate terrorism.

State faces a number of challenges to its passport fraud detection efforts, and these challenges make it more difficult to protect U.S. citizens from terrorists, criminals, and others. Information on U.S. citizens listed in the federal government's consolidated terrorist watch list is not systematically provided to State. Moreover, State does not routinely obtain from the Federal Bureau of Investigation (FBI) the names of other individuals wanted by federal and state law enforcement authorities. We tested the names of 67 federal and state fugitives and found that 37, over half, were not in State's Consular Lookout and Support System (CLASS) database for passports. One of those not included was on the FBI's Ten Most Wanted list. State does not maintain a centralized and up-to-date fraud prevention library, hindering information sharing within State. Fraud prevention staffing reductions and interoffice workload transfers resulted in fewer fraud referrals at some offices, and insufficient training, oversight, and investigative resources also hinder fraud detection efforts.

Any effect that new passport examiner performance standards may have on State's fraud detection efforts is unclear because State continues to adjust the standards. State began implementing the new standards in January 2004 to make work processes and performance expectations more uniform nationwide. Passport examiner union representatives expressed concern that new numerical production quotas may require examiners to "shortcut" fraud detection efforts. However, in response to union and examiner concerns, State eased the production standards during 2004 and made a number of other modifications and compromises.

Crimes Suspected of 37 Federal and State Fugitives Not in CLASS Who Were Included in Our Test

Type of crime	Federal fugitives	State fugitives
Murder	5	4
Felonious assault and related acts	2	7
Child sex offenses	4	1
Drug trafficking	3	
Attempted murder	1	1
Bombings	1	
Child kidnapping		1
Other crimes	4	3
Total	**20**	**17**

Sources: State Department and other federal agencies.

Madam Chairman and Members of the Committee:

I am pleased to be here today to discuss our report on the State Department's efforts to strengthen U.S. passport fraud detection.[1]

Maintaining the integrity of the U.S. passport is essential to the State Department's effort to protect U.S. citizens from terrorists, criminals, and others. The department issued about 8.8 million passports in fiscal year 2004. Each year, State passport examiners refer tens of thousands of applications they suspect may be fraudulent to their local fraud prevention offices. In fiscal year 2004, State's Diplomatic Security Service arrested about 500 individuals for passport fraud and about 300 were convicted. Passport fraud is often intended to facilitate such crimes as illegal immigration, drug trafficking, and alien smuggling.

Our report addressed three key issues: (1) how passport fraud is committed, (2) what key challenges State faces in its fraud-detection efforts, and (3) what effect new passport examiner performance standards could have on fraud detection. Today I am going to focus my discussion on the first two issues, and I will also discuss our recommendations to State and State's response to them.

For our work on this subject, we reviewed various fraud statistics and investigative case files maintained by relevant State bureaus and observed State's fraud detection efforts at 7 of the 16 domestic passport-issuing offices. We also tested State's use of electronic databases for fraud detection and interviewed officials in various State offices and bureaus involved in this issue. We conducted our work from May 2004 to March 2005 in accordance with generally accepted government auditing standards.

Summary

We found that identity theft is the primary tactic used by individuals fraudulently applying for U.S. passports. Specifically, imposters' use of other people's legitimate birth and other identification documents accounted for 69 percent of passport fraud detected in fiscal year 2004, while false claims of lost, stolen, or damaged passports and other methods accounted for the remaining 31 percent. According to State's Bureau of Diplomatic Security, passport fraud is often committed in connection with other crimes, including narcotics trafficking, organized crime, money laundering, and alien smuggling. Fraudulently obtained passports help enable criminals to hide their movements and activities, and concerns exist that fraudulently obtained passports could also be used to support terrorism. U.S. passports allow their holders to enter

[1] U.S. Government Accountability Office, *State Department: Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts,* GAO-05-477, (Washington, D.C.: May 20, 2005)

the United States with much less scrutiny than is given to foreign citizens and also allow visa-free passage into many countries around the world, providing obvious potential benefits to terrorists and criminals operating on an international scale.

Our report details a number of challenges to State's passport fraud detection efforts, including information sharing deficiencies and insufficient fraud prevention staffing, training, oversight, and investigative resources. These challenges make it more difficult to protect U.S. citizens from terrorists, criminals, and others who would harm the United States. Specifically, State does not currently receive information on U.S. citizens listed in the Terrorist Screening Center (TSC) database, which is the federal government's consolidated terrorist watch list, nor does State routinely obtain from the FBI the names of individuals wanted by both federal and state law enforcement authorities. Therefore, many of these individuals are not listed in State's Consular Lookout and Support System (CLASS) name-check database for passports,[2] and they could obtain passports and travel internationally without the knowledge of appropriate authorities. We tested the names of 67 different federal and state fugitives—some wanted for serious crimes, including murder and rape—and found that fewer than half were in State's system. One of those not included was on the FBI's Ten Most Wanted list. Though State, TSC, and the FBI began exploring options for more routine information sharing on certain passport-related matters in mid- to late 2004, such arrangements are not yet in place.

In addition, State does not maintain a centralized electronic fraud prevention library that enables information sharing on fraud alerts, lost and stolen birth and naturalization certificates, counterfeit documents, and other fraud prevention resources. Further, we found that fraud prevention training is provided unevenly at different passport-issuing offices, some examiners have not had formal fraud prevention training in years, and training and oversight of passport acceptance agent operations are even more sporadic. State does not have any way of tracking whether many acceptance agent employees are receiving required training, it makes oversight visits to only a limited number of acceptance facilities each year, and it does not maintain records of all of the individuals accepting passport applications at those facilities, posing a significant fraud vulnerability.

Any effect that new passport examiner performance standards may have on State's fraud detection efforts is unclear because State continues to adjust the standards. State began implementing the new standards in January 2004 to make work processes and performance expectations more uniform nationwide. Passport examiner union representatives expressed concern that new numerical production quotas may require examiners to "shortcut" fraud detection efforts. However, in response to union and examiner concerns, State eased the production standards during 2004 and made a number of other modifications and compromises.

---

[2]State maintains a separate CLASS database for visas. References to CLASS throughout this testimony relate to the CLASS database for passports only.

We are recommending that State, as it works to improve the coordination and execution of passport fraud detection efforts, take several actions to improve and expedite information sharing, specifically by ensuring that State's CLASS system for passports contains a more comprehensive list of individuals identified in the Terrorist Screening Center database as well as state and federal fugitives, and by establishing and maintaining a centralized electronic fraud prevention library. We are also recommending that State consider designating additional positions for fraud prevention coordination and training in some domestic passport-issuing offices; examine the impact of other workload-related issues on fraud prevention; and strengthen its fraud prevention training and acceptance agent oversight programs. In commenting on a draft of this report, State generally concurred with our findings and conclusions. State indicated that it has already begun taking, plans to take, or is considering measures to address most of our recommendations.

Background

A U.S. passport is not only a travel document but also an official verification of the bearer's origin, identity, and nationality. Under U.S. law, the Secretary of State has the authority to issue passports. Only U.S. nationals[3] may obtain a U.S. passport, and evidence of citizenship or nationality is required with every passport application. Federal regulations list those who do not qualify for a U.S. passport, including those who are subjects of a federal felony warrant.

State Passport Operations

The Deputy Assistant Secretary for Passport Services oversees the Passport Services Office, the largest component of State's Consular Affairs Bureau. Passport Services consists of three headquarters offices: Policy Planning and Legal Advisory Services; Field Operations; and Information Management and Liaison. Also within Consular Affairs is the Office of Consular Fraud Prevention, which addresses passport, visa, and other types of consular fraud; the Consular Systems Division, responsible for the computer systems involved in passport services and other consular operations; and the Office for American Citizens Services, which handles most issues relating to passport cases at overseas posts. The Bureau of Diplomatic Security is responsible for investigating individual cases of suspected passport and visa fraud. The State Department Office of the Inspector General (OIG) also has some authority to investigate passport fraud.

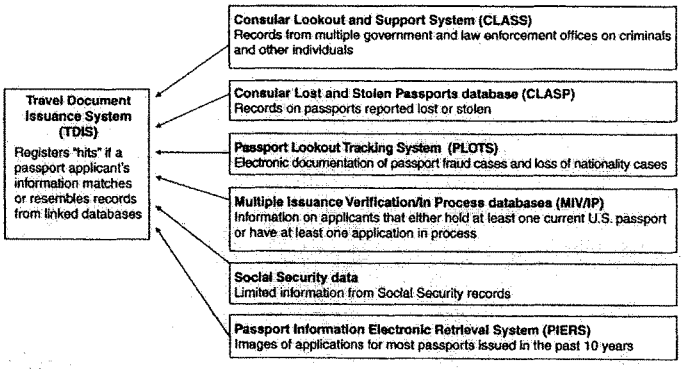
State operates 16 domestic passport-issuing offices, which employ approximately 480 passport examiners who approve and issue most U.S. passports that are printed each year. The number of passports issued by domestic passport offices has risen steadily in recent years, increasing from about 7.3 million in fiscal year 2000 to 8.8 million in fiscal year 2004. Overseas posts deal with a much lower volume of passports by comparison, handling about 300,000 worldwide in fiscal year 2004.

[3]National means a citizen of the United States or a noncitizen owing permanent allegiance to the United States.

Passport Application and Approval Process

The majority of passport applications are submitted by mail or in-person at one of almost 7,000 passport application acceptance facilities nationwide.[4] The passport acceptance agents at these facilities are responsible for, among other things, verifying whether an applicant's identification document (such as a driver's license) actually matches the applicant. Then, through a process called adjudication, passport examiners determine whether they should issue each applicant a passport. Adjudication requires the examiner to scrutinize identification and citizenship documents presented by applicants to verify their identity and U.S. citizenship. The passport adjudication process is facilitated by computer systems, including the Travel Document Issuance System, which appears on passport examiners' screens when the adjudication begins and automatically checks the applicant's name against several databases. Figure 1 identifies the key computer databases available to help examiners adjudicate passport applications and detect potential fraud.

Figure 1: Electronic Databases Available to Passport Examiners



Source: State Department.

In addition, examiners scrutinize paper documents and other relevant information during the fraud detection process, watch for suspicious behavior and travel plans, and request additional identification when they feel the documents presented are insufficient. When examiners detect potentially fraudulent passport applications, they send the applications to their local fraud prevention office for review and potential referral to State's Bureau of Diplomatic Security for further investigation.

[4]Number is as of March 2005. State officials noted that this number changes frequently as new acceptance facilities are added and others are dropped.

Identity Theft a Primary Means of Committing Fraud

State's Bureau of Diplomatic Security investigators stated that imposters' use of assumed identities, supported by genuine but fraudulently obtained identification documents, was a common and successful way to fraudulently obtain a U.S. passport. This method accounted for 69 percent of passport fraud detected in fiscal year 2004. Investigators found numerous examples of aliens and U.S. citizens obtaining U.S. passports using a false identity or the documentation of others to hide their true identity. In one example, in 1997, a naturalized U.S. citizen born in Cuba stole a Lear jet and transported it to Nicaragua. At the time of his arrest in 2003, he was using an assumed identity and possessed both false and legitimate but fraudulently obtained identification documents, including a U.S. passport in the name he used while posing as a certified pilot and illegally providing flight instruction. Seized at his residence when he was arrested were two Social Security cards, four driver's licenses, three Puerto Rican birth certificates, one U.S. passport, one pilot identification card, numerous credit cards and checking account cards, and items used to make fraudulent documents. In October 2004, he pled guilty to knowingly possessing five or more "authentication devices" and false identification documents, for which he was sentenced to 8 months confinement. In another case, a man wanted for murdering his wife obtained a Colorado driver's license and a passport using a friend's Social Security number and date and place of birth. Three and four years later he obtained renewal and replacement passports, respectively, in the same assumed identity. He was later arrested and pled guilty to making a false statement in an application for a passport. He was sentenced to about 7 months time served and returned to California to stand trial for murdering his wife.

Applicants commit passport fraud through other means, including submitting false claims of lost, stolen, or mutilated passports; child substitution; and counterfeit citizenship documents. Some fraudulently obtain new passports by claiming to have lost their passport or had it stolen or damaged. For example, one individual who used another person's Social Security number and Ohio driver's license to report a lost passport obtained a replacement passport through the one-day expedited service. This fraudulently obtained passport was used to obtain entry into the United States 14 times in less than three years. Diplomatic Security officials told us that another means of passport fraud is when individuals obtain replacement passports by using expired passports containing photographs of individuals they closely resemble. This method of fraud is more easily and commonly committed with children, with false applications based on photographs of children who look similar to the child applicant.[5] Assuming the identity of a deceased person is another means of fraudulently applying for a passport.

[5]In an effort to address this problem, State established a new requirement in February 2004 that children aged 14 and under appear with their parents when applying for a passport to allow comparison of the children to the photographs being submitted.

Passports Used to Commit Other Crimes

According to State Bureau of Diplomatic Security documents, passport fraud is often commited in connection with other crimes, including narcotics trafficking, organized crime, money laundering, and alien smuggling. According to Diplomatic Security officials, concerns exist within the law enforcement and intelligence communities that passport fraud could also be used to help facilitate acts of terrorism. Using a passport with a false identity helps enable criminals to conceal their movements and activities, and U.S. passports provide their holders free passage into our country with much less scrutiny than is given to foreign citizens. U.S. passports also allow visa-free passage into many countries around the world, providing obvious benefits to criminals operating on an international scale. According to State officials, the most common crime associated with passport fraud is illegal immigration. For example, one woman was recently convicted for organizing and leading a large-scale passport fraud ring that involved recruiting American women to sell their children's identities, so that foreign nationals could fraudulently obtain passports and enter the United States illegally. According to the Department of State, the woman targeted drug-dependent women and their children, paying them about $300 for each identity and then using the identities to apply for passports. The woman then sold the fraudulently obtained passports to illegal aliens for as much as $6,000 each.

State Faces Challenges to Fraud Detection Efforts

One of the key challenges to State's fraud detection efforts is limited interagency information sharing. Specifically, State currently lacks access to the Terrorist Screening Center's consolidated terrorist watch list database, which was created in 2003 to improve information sharing among government agencies. By consolidating terrorist watch lists, TSC is intended to enable federal agencies to access critical information quickly when a suspected terrorist is encountered or stopped within the United States, at the country's borders, or at embassies overseas. However, because State's CLASS name-check database does not contain the TSC information, U.S. citizens with possible ties to terrorism could potentially obtain passports and travel internationally without the knowledge of appropriate authorities.

Although TSC has been operational since December 2003, State and TSC did not begin exploring the possibility of uploading data from the TSC database into passport CLASS until December 2004. State and TSC have not reached an agreement about information-sharing, though State sent an official proposal to TSC in January 2005. A TSC official told us that she does not foresee any technical limitations, and added that TSC agrees that it is important to work out an agreement with State. We recommended that State and other parties expedite such arrangements, and State said that it and the TSC are actively working to do so.

CLASS Does Not Include Names of All Wanted Federal and State Fugitives

Because the FBI and other law enforcement agencies do not currently provide State with the names of all individuals wanted by federal law enforcement authorities,

State's CLASS name-check system does not contain the names of many federal fugitives, some wanted for murder and other violent crimes; these fugitives could therefore obtain passports and potentially flee the country. The subjects of federal felony arrest warrants are not entitled to a U.S. passport. According to FBI officials, FBI databases contain the names of approximately 37,000 individuals wanted on federal charges. State Department officials acknowledge that many of these individuals are not listed in CLASS. We tested the names of 43 different federal fugitives and found that just 23 were in CLASS; therefore, passport examiners would not be alerted about the individuals' wanted status if any of the other 20 not in CLASS applied for a passport. In fact, one of these 20 did obtain an updated U.S. passport 17 months after the FBI had listed the individual in its database as wanted. A number of the 20 federal fugitives who were included in our test and were found not to be in CLASS were suspected of serious crimes, including murder. One was on the FBI's Ten Most Wanted list. Table 1 lists the crimes suspected of the federal fugitives in our test.

Table 1: Crimes Suspected of 20 Federal Fugitives Not in CLASS Who Were Included in Our Test

Type of Crime	Number of fugitives
Murder	5
Felonious assault and related crimes	2
Child sex offenses	4
Drug trafficking	3
Attempted murder	1
Bombings	1
Other crimes	4

Sources: Various law enforcement agency databases and Web sites and the State Department's CLASS name-check system.

State officials told us that they had not initiated efforts to improve information sharing with the FBI on passport-related matters until the summer of 2004 because they had previously been under the impression that the U.S. Marshal's Service was already sending to CLASS the names of all fugitives wanted by federal law enforcement authorities. State officials were not aware that the information in the U.S. Marshal's database was not as comprehensive as that contained in the FBI-operated National Crime Information Center database. State officials became aware of this situation when the union representing passport examiners brought to their attention that a number of individuals on the FBI's Ten Most Wanted list were not in CLASS. In the summer of 2004, the FBI agreed to State's request to provide the names from the FBI's Ten Most Wanted list. As part of these discussions, State and the FBI explored other information-sharing opportunities as well, and FBI headquarters officials sent a message instructing agents in its field offices how to provide names of U.S. citizens who are FBI fugitives to State on a case-by-case basis.

Additionally, State began discussions with the FBI about receiving information on individuals with FBI warrants on a more routine and comprehensive basis.

According to FBI officials, State requested that the FBI provide only the names of FBI fugitives and not those of individuals wanted by other federal law enforcement entities. However, the FBI is the only law enforcement agency that systematically compiles comprehensive information on individuals wanted by all federal law enforcement agencies, and, according to FBI officials, it is the logical agency to provide such comprehensive information to State. We recommended that State expedite arrangements to enhance interagency information sharing with the FBI to ensure that the CLASS system contains a more comprehensive list of federal fugitives. According to State, it sent a written request on this issue to the FBI in April 2005. State also noted that it had reached agreement in principal with the FBI on information sharing efforts related to FBI fugitives.

In addition to its role in compiling information on federal fugitives, the FBI is also the only law enforcement agency that compiles comprehensive information on individuals wanted by state and local authorities. According to FBI officials, FBI databases contain the names of approximately 1.2 million individuals wanted on state and local charges nationwide. FBI officials told us that some of the most serious crimes committed often involve only state and local charges. We tested the names of 24 different state fugitives and found that just 7 were in CLASS; therefore, the CLASS system would not flag any of the other 17, were they to apply for a passport.[6] Table 2 lists the crimes suspected of the 17 tested state fugitives not in CLASS who were included in our test.

Table 2: Crimes Suspected of 17 State Fugitives Not in CLASS Who Were Included in Our Test

Type of Crime	Number of fugitives
Murder	4
Felonious assault and related crimes	7
Child sex offenses	1
Attempted murder	1
Child kidnapping	1
Other crimes	3

Sources: Various law enforcement agency databases and Web sites and the State Department's CLASS name-check system.

During our review, State Department officials told us that having a comprehensive list of names that included both federal and state fugitives could "clog" State's CLASS system and slow the passport adjudication process. They also expressed concern that the course of action required of State would not always be clear for cases involving passport applicants wanted on state charges. We recommended that State work with the FBI to ensure that the CLASS system contains a more comprehensive list of state fugitives. In commenting on a draft of our report, State said that it now

[6]We also noted that 10 of the 20 tested federal fugitives that were not in CLASS were also wanted on state charges. Thus, if State fugitives had been listed in CLASS, these individuals would have been flagged, even if information on their federal warrants had been missed.

intends to work with the FBI and U.S. Marshal's Service to establish an automated mechanism for integrating information on state warrants into CLASS.

Limited Intra-agency Information Sharing May Be Affecting Fraud Detection

State does not maintain a centralized and up-to-date electronic fraud prevention library, which would enable passport-issuing office personnel to efficiently share fraud prevention information and tools. As a result, fraud prevention information is provided inconsistently to examiners among the 16 domestic offices. For example, at some offices, examiners maintain individual sets of fraud prevention materials. Some print out individual fraud alerts and other related documents and file them in binders. Others archive individual e-mails and other documents electronically. Some examiners told us that the sheer volume of fraud-related materials they receive makes it impossible to maintain and use these resources in an organized and systematic way.

Other information sharing tools have not been effectively maintained. Consular Affairs' Office of Consular Fraud Prevention maintains a Web site and "e-room" with some information on fraud alerts, lost and stolen state birth documents, and other resources related to fraud detection, though fraud prevention officials told us the Web site is not kept up to date, is poorly organized, and is difficult to navigate. We directly observed information available on this Web site during separate visits to State's passport-issuing offices and noted that some of the material was outdated by as much as more than a year. The issuing office in Seattle developed its own online fraud library that included information such as the specific serial numbers of blank birth certificates that were stolen, false driver's licenses, fraud prevention training materials, and a host of other fraud prevention information resources and links. However, this library is no longer updated. Most of the 16 fraud prevention managers we talked to believed that the Bureau of Consular Affairs should maintain a centralized library of this nature for offices nationwide.

We recommended that State establish and maintain a centralized and up-to-date electronic fraud prevention library that would enable passport agency personnel at different locations across the United States to efficiently access and share fraud prevention information and tools. Commenting on our draft report, State said that it now intends to design a centralized online passport "knowledgebase" that will include extensive sections on fraud prevention resources.

Staffing Change Reduced Time Available to Review Fraud Cases

In January 2004, State eliminated the assistant fraud prevention manager position that had existed at most of its domestic passport-issuing offices, and most Fraud Prevention Managers believe that this action was harmful to their fraud detection program. State eliminated the position primarily to enable more senior passport examiners to serve in that role on a rotational basis to gain deeper knowledge of the subject matter and enhance overall fraud detection efforts when they returned to adjudicating passport applications. However, managers at 10 of the 12 offices that

previously had permanent assistants told us that the loss of this position had been harmful to their fraud detection program. In particular, managers indicated that the loss of their assistant impacted their own ability to concentrate on fraud detection by adding to their workload significant additional training, administrative, and networking responsibilities, while also diverting from their fraud trend analysis and preparation of reports and case referrals.

Fraud Prevention Managers and other State officials have linked declining fraud referrals to the loss of the assistant fraud prevention manager position. In the 12 offices that previously had permanent assistants, fraud referral rates from the managers to Diplomatic Security decreased overall by almost 25 percent from fiscal year 2003 through 2004,[7] the period during which the position was eliminated, and this percentage was much higher in some offices.[8] Without their assistants helping them screen fraud referrals, check applicant information, and assist with other duties related to the process, managers said they are making fewer fraud referrals to Diplomatic Security because they lack the time and do not believe they can fully rely on new rotational staff to take on these responsibilities.

We recommended that State consider designating additional positions for fraud prevention coordination and training in domestic passport-issuing offices. Passport Services management told us they were not planning to re-establish the permanent assistant role, but that they are in the process of filling one to two additional fraud prevention manager positions at each of the 2 offices with the largest workloads nationwide. State also plans to establish one additional fraud prevention manager position at another issuing office with a large workload. Commenting on our draft report, State said that it would now also consider rotating GS-12 Adjudication Supervisors through local fraud prevention offices to relieve Fraud Prevention Managers of some of their training responsibilities.

Interoffice Transfers of Passport Adjudication Workload Result, in Some Cases, in Fewer Fraud Referrals Back to Originating Office

State routinely transfers adjudication cases among the different offices to balance workloads, and Fraud Prevention Managers at a number of issuing offices said they had noticed a lower percentage of fraud referrals returned to them from the 3 offices that were assigned a bulk of the workload transfers. In fiscal year 2004, 28 percent of passport applications were transferred to 1 of these 3 offices for adjudication, while other issuing offices adjudicated 72 percent. Although these 3 offices received 28 percent of the applications, they provided only 11 percent of total fraud referrals to the originating agencies. For fiscal year 2003, the 3 processing centers adjudicated 26

[7]In the 4 offices that did not previously have permanent assistants, fraud referral rates decreased on average by only 7 percent during the same period.

[8]Two offices that had assistant fraud prevention managers in 2003 saw increases in their fraud referral rates. These 2 offices received just over 8 percent of the total applications received by offices that had assistants.

percent of the applications but provided only 8 percent of the fraud referrals. In 2004, 1 of the issuing offices transferred out to processing centers 63 percent of its applications (about 287,000) but received back from the processing centers only 2 percent of the fraud referrals it generated that year. In 2003, this office transferred out 66 percent of its workload while receiving back only 8 percent of its total fraud referrals.

Fraud Prevention Managers and other officials told us that one reason fewer fraud referrals return from these 3 offices is that passport examiners handling workload transfers from a number of different regions are not as familiar with the demographics, neighborhoods, and other local characteristics of a particular region as are the examiners who live and work there. For example, some officials noted that, in instances when they suspect fraud, they might telephone the applicants to ask for additional information so they can engage in polite conversation and ask casual questions, such as where they grew up, what school they attended, and other information. The officials noted that, due to their familiarity with the area, applicants' answers to such questions may quickly indicate whether or not their application is likely to be fraudulent. One examiner in an office that handled workload transfers from areas with large Spanish-speaking populations said that the office had an insufficient number of Spanish-speaking examiners, emphasizing the usefulness of that skill in detecting dialects, accents, handwriting, and cultural references that conflict with information provided in passport applications.

We recommended that State assess the extent to which and reasons why workload transfers from one domestic passport issuing office to another were, in some cases, associated with fewer fraud referrals and to take any corrective action that may be necessary. In its official comments on our draft report, State did not address this recommendation.

State Lacks Established Refresher Training; Such Training Is Provided Unevenly

State has not established a core curriculum and ongoing training requirements for experienced passport examiners, and thus such training is provided unevenly at different passport-issuing offices. While State recently developed a standardized training program for new hires that was first given in August, we reviewed the training programs and materials at all 7 issuing offices we visited and discussed the programs and materials at other offices with the remaining nine Fraud Prevention Managers by telephone and found that the topics covered and the amount and depth of training varied widely by office. Some had developed region-specific materials; others relied more heavily on materials that had been developed by passport officials in Washington, D.C., and were largely outdated. Some scheduled more regular training sessions, and others did so more sporadically. Several examiners told us they had not received any formal, interactive fraud prevention training in at least 4 years. Some Fraud Prevention Managers hold brief discussions on specific fraud cases and trends at monthly staff meetings, and they rely on these discussions to serve as refresher training. Some Fraud Prevention Managers occasionally invite officials from other government agencies, such as the Secret Service or DHS, to share

their fraud expertise. However, these meetings take place only when time is available. For example, officials at one issuing office said the monthly meetings had not been held for several months because of high workload; another manager said he rarely has time for any monthly meetings; and two others said they do not hold such discussions but e-mail to examiners recent fraud trend alerts and information.

We recommended that State establish a core curriculum and ongoing fraud prevention training requirements for all passport examiners. State said that it is implementing a standardized national training program for new passport examiners but that it is still providing training to existing passport examiners on a decentralized basis. State officials told us that they intend to develop a national training program for experienced examiners, after certain organizational changes are made in State's headquarters passport operation.

Sporadic Training and Limited Oversight of Acceptance Agents Constitute Significant Fraud Vulnerability

Numerous passport-issuing agency officials and Diplomatic Security investigators told us that the acceptance agent program is a significant fraud vulnerability. Examples of acceptance agent problems that were brought to our attention include important information missing from documentation and identification photos that did not match the applicant presenting the documentation. Officials at one issuing office said that their office often sees the same mistakes multiple times from the same acceptance facility. These officials attributed problems with applications received through acceptance agents to the sporadic training provided for and limited oversight of acceptance agents. State has almost 7,000 passport acceptance agency offices, and none of the 16 issuing offices provide comprehensive annual training or oversight to all acceptance agency offices in their area. Instead, the issuing offices concentrate their training and oversight visits on agency offices geographically nearest to the issuing offices, or in large population centers, or where examiners and Fraud Prevention Managers had reported problems, or in high fraud areas. Larger issuing offices in particular have trouble reaching acceptance agency staff. At one larger issuing office with about 1,700 acceptance facilities, the Fraud Prevention Manager said he does not have time to provide acceptance agent training and that it is difficult for issuing office staff to visit many agencies. A manager at another large issuing office that covers an area including 11 states said she does not have time to visit some agencies in less populated areas.

While State officials told us all acceptance agency staff must be U.S. citizens, issuing agency officials told us they have no way of verifying that all of them are. Management officials at one passport-issuing office told us that, while their region included more than 1,000 acceptance facilities, the office did not maintain records of the names of individuals accepting passport applications at those facilities.

We recommended that State strengthen its fraud prevention training efforts and oversight of passport acceptance agents. In commenting on a draft of our report, State said that it is adapting and expanding computer-based training for U.S. Postal

Service acceptance facilities for more widespread use among acceptance agents nationwide. State also indicated that it would institute a nationwide quality review program for its acceptance facilities. However, State officials recently told us that the quality reviews would focus only on new acceptance facilities and existing facilities with reported problems. It is unclear whether State will perform quality reviews for the rest of its nearly 7,000 facilities.

Overstretched Investigative Resources Hinder Fraud Detection

Although State's Bureau of Diplomatic Security has provided additional resources for investigating passport fraud in recent years, its agents must still divide their time among a number of competing demands, some of which are considered a higher priority than investigating passport fraud. A Diplomatic Security official told us that, after the September 11th terrorist attacks, the bureau hired about 300 additional agents, at least partially to reduce investigative backlogs.[9] Diplomatic Security and passport officials told us that, while the increased staff resources had helped reduce backlogs to some degree, agents assigned to passport fraud investigations are still routinely pulled away for other assignments. At most of the offices we visited, few of the agents responsible for investigating passport fraud were actually there. At one office, all of the agents responsible for investigating passport fraud were on temporary duty elsewhere, and the one agent covering the office in their absence had left his assignment at the local Joint Terrorism Task Force to do so. Agents at one office said that five of the eight agents involved in passport fraud investigations there were being sent for temporary duty in Iraq, as were many of their colleagues at other offices.

Agents at all but 2 of the 7 bureau field offices we visited said they are unable to devote adequate time and continuity to investigating passport fraud. We noted that the number of new passport fraud investigations had declined by more than 25 percent over the last five years, though Diplomatic Security officials attributed this trend, among other factors, to refined targeting of cases that merit investigation. The Special-Agent-in-Charge of a large Diplomatic Security field office in a high fraud region expressed serious concern that, in 2002, the Bureau of Diplomatic Security began requiring, to reduce backlog of old cases, that most cases be closed after 12 months, whether or not the investigations were complete. The agent said that about 400 incomplete cases at his office were closed. A Diplomatic Security official in Washington, D.C., told us that, while field offices had been encouraged to close old cases that were not likely to be resolved, there had not been a formal requirement to do so. State officials agreed that Diplomatic Security agents are not able to devote adequate attention to investigating passport fraud, and told us that the Bureau of Diplomatic Security plans to hire 56 new investigative agents over the next few years. According to State officials, these new investigators will be solely dedicated to investigating passport and visa fraud and will not be pulled away for other duty.

[9]State officials also noted that the Bureau of Consular Affairs funds more than 120 Diplomatic Security agent positions nationwide to help support efforts to investigate passport fraud.

Effect of New Examiner Performance Standards on Fraud Detection Remains Unclear

Although State's approach to developing new nationwide passport examiner production standards, implemented in January 2004, raises methodological concerns, subsequent changes to the standards make an assessment of their impact on fraud detection premature. State developed new nationwide passport examiner production standards in an effort to make performance expectations and work processes more uniform among its 16 issuing offices. However, State tested examiner production before standardizing the passport examination process; differences in work processes across offices at the time of the test limited the validity of the test results. State then used the results in conjunction with old standards to set new nationwide standards. The new standards put additional emphasis on achieving quantitative targets. Responding to concerns about their fairness due to changes that may have slowed the examination process, as well concerns that the new standards led examiners to take "shortcuts" in the examination process to meet their number targets, State made a number of modifications to the production standards during the year. The various modifications have made it unclear what impact the standards have had on passport fraud detection.

Madam Chairman, this completes my prepared statement. I would be happy to respond to any questions you or other Members of the Committee may have at this time.

Contacts and Acknowledgements

If you or your staff have any questions about this testimony, please contact Jess Ford at (202) 512-4128 or fordj@gao.gov, or Michael Courts at (202) 512-8980 or courtsm@gao.gov.

Individuals making key contributions to this testimony included Jeffrey Baldwin-Bott, Joseph Carney, Paul Desaulniers, Edward Kennedy, and Mary Moutsos.

(320360)

Statement of Michael Johnson
Former Special Agent in Charge, Miami Field Office, Diplomatic Security Service
United States Department of State
Before the U.S. Senate
Homeland Security and Governmental Affairs Committee
29 June 2005

"Vulnerabilities in the U.S. Passport System Can Be Exploited by Criminals and Terrorists"

I would like to thank Chairman Collins, Senator Lieberman, and all the other members of the committee for the opportunity to appear before you today. Passport fraud is a much misunderstood problem, and I am very pleased that the committee is holding this hearing to discuss how it affects our country's homeland security, including the possibility that weaknesses in the passport issuance regime could be exploited by terrorists.

For the record, my name is Michael Johnson. I served in the State Department's Bureau of Diplomatic Security for eighteen years. In 1999, I began serving in Diplomatic Security's Miami Field Office, rising to be its Special Agent in Charge in 2002 until I left at the end of 2004. I would like to add that while I am currently the Special Agent in Charge of the Miami Field Office of the Office of Export Enforcement in the Commerce Department, I am not here today testifying on their behalf.

As you know, the Department of State is the sole Executive Branch Department with the authority to issue passports to citizens of the United States. With this authority comes the responsibility to maintain the integrity of the United States passport. The Department's Bureau of Consular Affairs handles much of this responsibility, with the task of supporting its mission falling to the Bureau of Diplomatic Security's criminal investigative programs. Investigating passport fraud is just one of Diplomatic Security's responsibilities, which also include protecting the Secretary of State and high-ranking foreign dignitaries and officials visiting the United States; protecting U.S. embassies and consulates abroad; conducting personnel security investigations; and training foreign civilian law enforcement officers to protect their countries from terrorism.

As Special Agent in Charge of Diplomatic Security's Miami Field Office, I was charged with overseeing what has historically been Diplomatic Security's busiest field office. I believe this places me in a unique position to discuss efforts to combat passport fraud.

Possession of a U.S. passport is important because it allows an individual to prove two things: United States citizenship and identity. In fact, it is the only official government document that establishes both, making the U.S. passport the most widely accepted and versatile government-issued document in the United States. Most consider it the "gold standard" of all passports, and, as a result, it can be used throughout the world to establish bank accounts and credit accounts; to cash checks; apply for driver's licenses or welfare and unemployment; and any other activity requiring an individual to prove citizenship or identity.

The large majority of all passport fraud cases involve false claims to U.S. citizenship. The exceptions are those cases in which the false applicants are already U.S. citizens and their motive for committing passport fraud is the assumption of a new identity. But it is the potential for a non-U.S. citizen to obtain sham-U.S. citizenship through a false passport application that sets this crime apart from others. Barring the issuance of a naturalization certificate based on false information, there is simply no other crime that allows an individual to hide their true identity, citizenship, and, most importantly, the true motives behind committing such an act. Given the post-9/11 scrutiny placed on non-U.S. citizens inside the United States, stopping passport fraud is at the core of strong border and homeland security procedures.

When discussing the problems posed by passport fraud, we should remember that the U.S. passport is an extraordinarily difficult document to counterfeit or to fraudulently modify. Unfortunately, the same cannot be said for documents used to establish eligibility for a passport. The threat to the passport comes when bogus versions of these documents, called "breeder documents," are used in the passport application process to falsely establish an applicant's citizenship or nationality and proof of identity. Key among these breeder documents are bogus birth certificates. Weaknesses in these documents can provide unscrupulous individuals a backdoor method of acquiring a U.S. passport.

Making matters worse is that often these breeder documents are provided by organized rings of criminals who understand the passport application process and the value these documents have. These individuals are not particular about who buys their breeder documents. In fact, I believe that, given the opportunity, they would not hesitate to sell them to terrorists.

During my years in the Miami Field Office, we investigated a number of organized fraud rings. These often involved the sale of Puerto Rican birth certificates because of the few, if any, controls on the document. For example, in 2001 and 2002 approximately 6000 blank Puerto Rican birth certificates were stolen from Puerto Rican government offices. Within a short period of time those blanks began showing up around the United States, many in support of applications for U.S. passports. We arrested several people who attempted to use these fraudulent birth certificates but never made any major headway in finding the illegal document vendors.

Despite the challenge posed to the integrity of the United States passport, I do not believe that enough is being done to protect this vitally important document. In my experience, DSS thinks of itself primarily as a security service and tends to view passport fraud as a less important part of its mission. Historically, passport fraud has been viewed primarily as an immigration problem, with little impact on national or homeland security. Recently, though, it has become increasingly clear that passport fraud is more than just an immigration crime.

There are two common misperceptions about passport fraud that I would like to clear up. First, passport fraud is not primarily committed to facilitate illegal immigration. In fact, the overwhelming majority of passport fraud cases involve applicants who are already in the United States. By obtaining a U.S. passport by utilizing bogus breeder documents, an unscrupulous individual will have a document that allows its holder to travel into and out of the United States freely, bypassing the border requirements for non-U.S. citizens. It is also provides ironclad proof

of an individual's identity. The value of this document to an individual trying to conceal their identity or blend in to American society is obvious.

Passport fraud is also a wholly different crime from identity theft. In fact, in my experience individuals will often sell their identity to fraud rings to be resold to others who wish to assume their identity for nefarious purposes. Selling one's identity is often done by those with a need for quick cash, such as drug users, and they often remain unaware of how their identity was ultimately used. While there is no question that identity theft may be a component of passport fraud, there are just as many passport fraud cases where no identity theft has occurred and the individual has willingly sold their identity. There have also been numerous passport fraud cases in which identities have been willingly loaned, usually in the form of a birth certificate, to facilitate the illegal entry of foreign nationals, often children, into the United States. Other times, suspects may use fraudulent or counterfeit birth certificates, and essentially create the identity of someone that has never existed.

Individuals committing passport fraud are no longer restricted to illegal aliens seeking economic refuge in the United States. Instead, passport fraud is being increasingly used to further a variety of other crimes, both violent and non-violent, such as drug-trafficking, money laundering, and social security fraud. As a result, punishing and deterring passport fraud can be a key tool in combating a variety of crimes. Unfortunately, more needs to do be done to make this tool effective.

One example of the kind of tactics we need to combat passport fraud can be found in an operation initiated by the Miami Field Office – "Operation Global Pursuit."

In late 2001, following 9/11, the Miami Field Office entered into an agreement with the U.S. Attorney's Office for the Southern District of Florida regarding the prosecution of fraud cases at the Miami International Airport. At the time, the Immigration and Naturalization Service was only seeking the federal prosecution of a limited number of the more than three hundred fraud cases uncovered every month at the Miami Airport immigration port of entry. This informal agreement between the DSS's Miami Field Office and the U.S. Attorney authorized the DSS prosecution of 25 to 30 visa and passport fraud cases per month originating at the Miami Airport. The primary goal of this operation was to gather intelligence on the sources of the counterfeit travel documents by prosecuting the individuals who used them. This was to be the means to gain the cooperation needed to obtain this intelligence. The information from these end-users would eventually be used to identify and prosecute, either outside the U.S. or in the Southern District of Florida, individuals involved in the manufacture or sale of counterfeit U.S. visas and passports.

Over the next six months, various bureaucratic issues between the three agencies delayed the start of the operation. Finally, in July 2002, DSS Miami Field Office agents began working with INS Inspectors and made the first arrests under Operation Global Pursuit. Between July and December 2002, Miami Field Office agents made 29 arrests at the Miami Airport. From those 29 arrests, agents obtained preliminary intelligence relating to the possible identification of document vendors in several countries.

Unfortunately, in January 2003, the cooperation from INS at the Miami Airport came to a virtual standstill as the agency prepared to transfer to the new Department of Homeland Security. In June 2003, the US Attorney interceded on behalf of the Miami Field Office and instituted prosecution procedures that required the new Bureau of Customs and Border Protection (CBP) to fully cooperate in this initiative. This action also led to a new local agreement between CBP, Immigration and Customs Enforcement, and the Miami Field Office to fully cooperate in Operation Global Pursuit.

During the operation, we found that most suspects, including those who were initially cooperative, refused to cooperate once they discovered the low sentences they would receive. In fact, of the 30 individuals convicted under Operation Global Pursuit as of April 2003, only one received a sentence greater than 90 days, and over two-thirds received sentences of 60 days or less.

The story of Operation Global Pursuit illustrates two important points: first, penalties for passport fraud are insufficient to punish or deter the crime. Second, efforts like Operation Global Pursuit require coordination across the federal government among numerous federal agencies, agencies that often possess overlapping jurisdictions. As a result, strong leadership is essential for the success of operations to combat passport fraud.

Devoting sufficient resources to the problem is also essential to fighting passport fraud. While the DSS is filled with high quality people, sadly, most are not given enough time to develop a specialization in investigating passport fraud.

Field offices are where most agents get their initial on-the-job training. DSS agents are assigned to field offices for two year tours of duty, primarily investigating passport fraud, before being reassigned, often after 18 months or less. As a result, agents are moved to other offices and other assignments just when they begin to develop some expertise in the subject matter and in the area in which they are stationed. I went through three such cycles when I was at the Miami Field Office. As a result, I found that I was constantly starting over with agents who had no experience investigating passport fraud and little experience in the area to which they were assigned. Often, breaks in an investigation will result from both deep experience in a geographic area and extensive knowledge of a subject matter. Too often, I found that good agents simply were not given enough time to develop the experience needed to effectively combat passport fraud.

One way to solve this problem would be to assign Diplomatic Security agents investigating passport fraud to offices on a permanent basis. This would give them the time needed to develop sufficient expertise to effectively combat passport fraud and would develop a cadre of agents with the expertise to take down the fraud rings that are attacking the integrity of the United States passport.

Another significant obstacle in combating passport fraud is that Diplomatic Security lacks an analytic capacity. During my service in the DSS, I found that there was simply no institutional capacity to spot and understand trends, analyze information gained from operations, and share intelligence across the DSS and other law enforcement organizations. The lack of such an

intelligence capacity cripples DSS's ability to identify and dismantle organizations across the world that are involved in the manufacture and sale of counterfeit documents used to illegally enter and or remain in the United States.

I again want to thank the committee for holding this hearing and I am now prepared to answer your questions.

U.S. Senate Homeland Security and Government Affairs Committee

Hearing on GAO Report 05-477,
"Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts"

Testimony of Frank E. Moss
Deputy Assistant Secretary for Passport Services
Bureau of Consular Affairs
U.S. Department of State

June 29, 2005

Chairman Collins, Ranking Member Lieberman, Distinguished Members of the Committee:

I am pleased to be here today to discuss what the State Department is doing to respond to the concerns raised by the Government Accountability Office in its Report entitled "Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts." I want to thank the GAO and especially their lead examiner, Michael Courts, for their hard work on this project. As the GAO report recognizes, the Department of State is already engaged in many areas to protect the integrity of the U.S. passport, working hand-in-hand with the State Department's Diplomatic Security Service, and with elements of the Homeland Security and Justice Departments. Still, we acknowledge that it is always possible to improve, and welcome GAO's observations and suggestions.

The integrity of the passport rests upon three major elements: the quality of the adjudication process, the security features of the passport itself, and the introduction of biometrics to make certain that the passport can only be used by the person to whom it is issued. Taken together, these elements constitute a comprehensive approach to passport security. Securing the document and the adjudication process is particularly important in an era when terrorists, transnational criminals and others seeking to enter the U.S. illegally view travel documents as valuable tools. By making sure that U.S. passports are only issued to American citizens, that they are more difficult to counterfeit and that the bearer of the passport is the same person

to whom the passport was issued, the Department of State actively enhances the security of this nation, while we continue to promote our international engagement through personal, commercial, educational and research exchanges with other nations.

During the last fiscal year the Department of State processed a total of 8.8 million U.S. passport applications. This set a record, exceeding the total from the previous year by more than one million applications and representing a workload increase of some 22 percent. This year, the Department of State is experiencing a 14 percent rise. So far in FY-2005, the Department has already processed more than 7 million passport applications and we are on track to adjudicate more than 10 million passports by the end of the fiscal year. This means that overall passport demand will have increased by approximately 40 percent in just two years.

As the Department of State develops plans to address the increase in demand for U.S. passports resulting from normal growth in international travel, their use by Americans, especially recently naturalized citizens, as portable proof of identity and nationality, and the Western Hemisphere Travel Initiative, we are dedicated to actively pursuing initiatives to improve the integrity of the U.S. passport. I would like to give you an overview today of what we have done and are doing to improve passport integrity.

Strengthening the Adjudication Process

A key objective is to ensure that U.S. passports are issued only to persons who are entitled to them. This process begins with a careful examination of identity and citizenship documentation, especially birth and naturalization certificates. Increased information sharing, both within the United States Government and with its partners overseas, is one of the most effective ways to strengthen this process so that only those entitled to U.S. citizenship receive a U.S. passport. This is a critical element in our strategy to "look behind the paper" in terms of passport adjudication.

The Department of State has actively worked to establish data exchange programs with other Federal agencies, as well as organizations like INTERPOL, in a manner that is mutually beneficial and that will keep U.S. passports out of the hands of those who are not eligible to receive them. For example, in April 2004, the Department signed a memorandum of understanding with the Social Security Administration (SSA) that would

permit the Department to verify the Social Security numbers of U.S. passport applicants. This measure provides another verification tool for passport specialists and consular officials adjudicating passport applications by allowing them to correlate the data provided by a passport applicant with information in SSA's system and use this information to support decisions about an applicant's identity. This initiative has now "gone live" at our passport agency here in Washington and will be operational nationwide by early August.

The Department has a long-standing and effective working relationship with federal law enforcement agencies that targets passport applicants of particular concern. Today, we have nearly 50,000 names of fugitives or other individuals of interest to law enforcement in the passport lookout system. Half of these were entered individually as a result of our outreach efforts. The other half of these entries are based on U.S. Marshals Service (USMS) federal fugitive warrants, data that the Department took the initiative to obtain.

To complement the USMS information, work is well underway to add to the passport lookout system an extract of FBI fugitive warrants from the NCIC Wanted Persons File. I am glad to report that last week we received a letter from the FBI that responds positively to our request for access to information on an additional group of persons subject to federal warrants who are sought by other federal law enforcement agencies. In addition, this positive response from the FBI may also open the door to access comprehensive information on persons subject to state and local warrants. Right now, we rely on the voluntary information exchange with law enforcement officials at the state and local levels which we have promoted through the sending of a letter from the Assistant Secretary of State for Consular Affairs to all the states' attorneys general. Having access to NCIC data would be far more desirable.

In 2004, the Department reached an agreement with INTERPOL to provide the Department's lost and stolen passport database to that organization via the U.S. National Central Bureau (NCB). The NCB shares the data with INTERPOL, which in turn makes this information available to all INTERPOL member states. The U.S. lost and stolen passport database currently contains the passport numbers of over 661,000 U.S. passports, that is, nearly 10 percent of the INTERPOL database. It is important to note that once a U.S. passport is reported lost or stolen, it is no longer valid for travel.

The Department of State is about to sign an agreement with the Terrorist Screening Center (TSC) that will provide information on American citizens who are of concern to TSC due to a nexus to terrorism or an ongoing investigation. This datashare program will enable the Terrorist Screening Center to learn of the passport application of an individual of interest and, under appropriate circumstances, take law enforcement action.

In addition, the Department of State provides to the National Counter Terrorism Center (NCTC) access to the Passport Records Imaging System Management (PRISM). This database includes scanned images of all passport applications since 1994.

Maintaining an aggressive fraud prevention program is another important element in safeguarding the adjudication process. The Department of State has undertaken a comprehensive review of its fraud prevention efforts and implemented a number of initiatives, including organizational improvements, enhanced training, regulatory changes, new tools, and new programmatic activities with domestic and international partners. All senior passport specialists now rotate through the fraud prevention office at domestic passport facilities to give them specialized experience in fraud detection. We see this effort as being crucial in helping to ensure that the specialized information and knowledge available in the Fraud Prevention Program office is available to passport specialists. Let me be clear—it is passport examiners who serve as the first line of defense against passport fraud. We are committed to giving them and their supervisors all appropriate tools to help them fulfill that responsibility. We see this rotational program as a key element in that effort.

The "lessons learned" from fraud investigations also directly influences our regulatory practices. To help prevent international child abduction, we now require that both parents consent to the issuance of a passport for a child. We also now mandate the presence of children under the age of 14 when passport applications are executed on their behalf. We are also making greater use, with the appropriate respect for privacy concerns, of commercial databases to assure that persons applying for passports are who they claim to be. Finally, we are conducting unannounced audits of passport agencies to review applications for proper adjudication, consistency and attention to fraud indicators. Results of these unannounced audits suggest to me that our anti-fraud strategy is effective; based on results

from eight agencies, we have a rate of about 1.76 percent in which non-serious errors were made by passport specialists in documenting passport applications. This is, of course, an opportunity for retraining our staff. The rate of potentially serious frauds identified through this validation study is far lower, running based on our preliminary results at about 3 per 10,000 passport applications.

The focus on fraud prevention is already paying dividends. Statistics for this fiscal year show an increase in referrals to fraud prevention offices, as well as an increase in the referral of presumptive fraud cases to the Department's Bureau of Diplomatic Security (DS) for further investigation. The Bureau of Consular Affairs enjoys excellent cooperation and support from DS, which has the responsibility for criminal investigations involving passport fraud. The statistics about the efficacy of joint Consular Affairs-Diplomatic Security efforts are compelling. So far in fiscal year 2005, DS opened 2,401 passport investigations and made 375 arrests; this represents a significant increase over the same period in 2004, when DS opened 1,722 cases and made 183 arrests.

Strengthening The Security of the Passport

Efforts to strengthen the adjudication process and augment fraud prevention efforts would be less effective if we did not attend to the other key elements of passport security with equal fervor. Turning to the passport itself, the Department recently completed the first cover-to-cover redesign of the document in more than a decade. The new passport includes a host of new security features, including sophisticated new fraud-resistant artwork, adopting printing techniques used in the current generation of U.S. currency, and other changes that significantly increase the physical security of the U.S. passport.

Our objective in designing the new passport is to further raise the bar against counterfeiting or the fraudulent use of lost or stolen passports. Advances including color shifting ink, microprinting, latent image lettering and a security laminate over the biographic data page that includes optical variations, all serve to deter counterfeiters and forgers. The biographic data page is being relocated from the inside of the front cover to the first inside page for added security. The inventory control number for each book is now the same as the passport number. Imagery on the inside pages of the passport incorporates more colors, stylized depictions of iconic American

scenes, and includes famous quotations from American history. The new passport, combined with security enhancements in the adjudication process, helps to ensure that only qualified applicants receive U.S. passports.

I am happy to share with the members of the Committee samples of the new passport.

Strengthening Passport Integrity Through Use of Biometrics

This next generation of U.S. passport, the e-passport, includes biometric technology that will further support the Government's border security goals. Without question, biometrics will strengthen U.S. border security by ensuring that the person carrying a U.S. passport is the person to whom the Department of State issued that passport.

Consistent with globally interoperable biometric specifications adopted by the International Civil Aviation Organization (ICAO) in May 2003, the United States has adopted the facial image as the first generation of biometric identifiers. The new U.S. passport includes a contactless chip in the rear cover of the passport that will contain the same data as that found on the biographic data page of the passport, including a digital image of the bearer's photograph. This data includes the following information about the bearer: the photograph, the name, the date and place of birth, as well as the passport number and the date of issuance and expiration all of which is protected by a unique encrypted signature. Looking to the future, the Department decided to require 64 KB of writeable memory on the contactless chip in the event that we subsequently decide to introduce additional biometrics. Should the United States Government decide to change the biometric requirements, this change will be subject to vetting through the Federal Register process.

On June 15, the Department, partnering with the Department of Homeland Security and in collaboration with Australia and New Zealand, launched an operational field test to measure the overall performance of the e-passport, issuing approximately 250 U.S. e-passports to personnel employed by United Air Lines and who fly internationally to or from Los Angeles. The Department of Homeland Security has developed separate lanes and installed e-passport readers to test their efficiency. Later this year, we will expand this pilot program to include diplomatic and official passports, with national deployment of the e-passport scheduled for 2006.

The Department of State is well aware of concerns that data written to the contactless chip in the e-passport may be susceptible to unauthorized reading. To help reduce this risk, anti-skimming materials that prevent the chip from being read when the passport book is closed or mostly closed will be placed in the passport.

The Department is confident that the new e-passport, including biometrics and other improvements, will take security and travel facilitation to a new level. Naturally, the Department will comprehensively test the operation and durability of the e-passport and work to resolve any issues as they occur. In fact, the Department of State is engaged in a continuous product improvement effort with regard to the U.S. passport. We will continue to monitor technical developments and help conduct research to ensure that we produce a passport that is highly secure, tamper resistant and globally interoperable.

The GAO's Recommendations

As I mentioned above, the passport name clearance system contains over 50,000 entries of persons wanted at the Federal, state and local levels. We agree with the GAO that enhanced interagency datasharing can improve that system significantly. Some of the need can be met almost immediately, while other aspects will require systems and program development. But we are well on the way to filling a gap in the system. As I said earlier, we are in the final stages of completing an MOU with the Terrorist Screening Center that will result in their U.S. Persons database being added to the Passport name check system.

GAO recommends the development and deployment of a national fraud library of suspect documents to allow our staff nationwide to efficiently access and share fraud prevention information and tools. Presently, there are several different resources that provide such information and we agree that finding a way to bring them together is desirable. An option we are pursuing in this regard is the U.S. Secret Service's (USSS) Questionable ID Documents (QID) database, which includes a section on valid documents, one on stolen documents and another on counterfeits and alterations. We are working with the Secret Service to obtain access to this database. An advantage of this system is the fact that we can contribute to

their database, and in doing so, assist them in their mission, while also avoiding significant development costs. We are also working to obtain electronic authentication of driver's licenses while also allowing the states access to passport data to help them verify the identity of their applicants.

The GAO recommends designating additional positions for fraud prevention coordination and training in domestic passport issuing offices, and establishing a more formalized fraud prevention training regimen. We agree, and have taken several steps to make this a reality. We are in the process of adding more Fraud Prevention Managers to the staffs of our larger agencies, and we have increased the numbers of persons working in the fraud offices, as well as the length of time they spend there. This will have a direct impact on improving the training that is provided to the Passport Specialists who adjudicate passport applications. Finally, under a Headquarters reorganization nearing completion, we are adding to the staff that coordinates and backstops the Fraud Prevention operations in the field agencies. Part of the work of the expanded Headquarters staff will be to develop a national fraud training program for the Specialists.

GAO looked at the issue of workload transfers from one domestic agency to another, which we do to make the best use of our issuance capabilities system-wide and because most of our work flows through a fee depository process. A theoretical risk in having applications from one region of the country adjudicated in another is missed opportunities to identify fraud because of a lack of familiarity with citizenship evidence from the originating region. We believe that we successfully address this risk through our selection of highly skilled Fraud Program managers, by rotating our senior passports specialists through the FPM office so that they can then assist and better train their staff, and by training centrally all of our newly hired specialists.

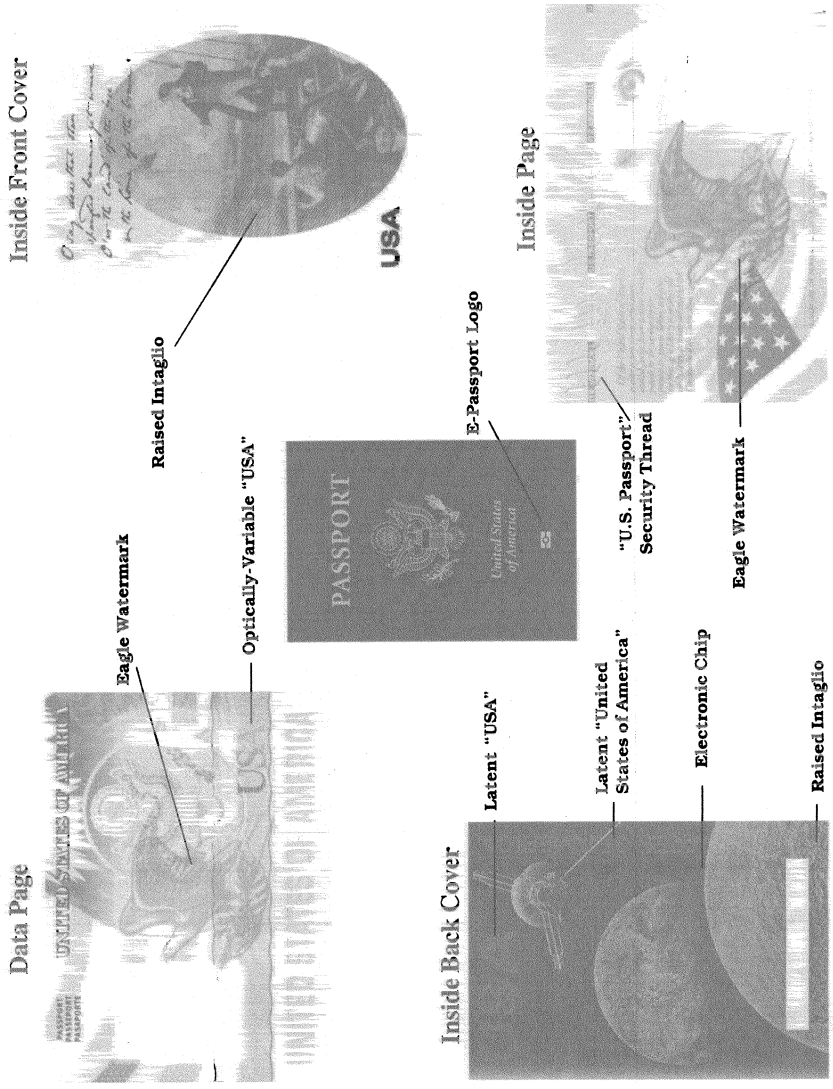
Finally, the GAO suggested increasing training and oversight of the 7,000-plus passport application acceptance agents nationwide, principally Postal Service employees and clerks of court, which perform the valuable service of accepting applications from U.S. citizens and in doing so bring the passport application process to the our citizens. In addition to being our representatives, they are the first line of defense in that they identify the passport applicant as the person he or she claims to be. Improved training is already underway through use of Computer Based Training (CBT) modules that have been developed in cooperation with the US Postal Service. Those

modules are also being adapted for use by other facilities. There are also initiatives in process to more closely monitor the quality of the work received from the acceptance agents.

Madam Chairman, I am grateful for the opportunity today to share with you the Department of State's comprehensive approach to enhancing U.S. border security by augmenting the security of all aspects of the U.S. passport program. Again, we appreciate GAO's constructive recommendations and look forward to working with Congress and the GAO to produce the most secure passport possible. At this time, I am happy to answer any questions you, the Ranking Member and the other distinguished members of the Subcommittee might have about the Department's fraud prevention efforts or the other facets of the U.S. passport program that I have discussed.

Strengthening U.S. Passport Security
Biometrics
Passport
Adjudication

Passport Lookout Database
Deadbeat Parent
88%
Fraud
3%
NonCitizen
3%
Loss of Citizenship
2%
Other
4%
Other includes:
Parental Custody
Repatriation
Marshal Warrant
Claim of Citizenship
Insufficient Evidence
Deceased
Passport Problems
Renunciation of Citizenship
Agency/Office/Individual
Requesting Catch Card
Attempted Renunciants
Indebtedness to Government
INS
Etc.


Data Page
Eagle Watermark
Optically-Variable "USA"
Inside Front Cover
Raised Intaglio
USA
PASSPORT
United States of America
E-Passport Logo
Inside Page
"U.S. Passport" Security Thread
Eagle Watermark
Inside Back Cover
Latent "USA"
Latent "United States of America"
Electronic Chip
Raised Intaglio

STATEMENT OF DONNA A. BUCELLA
DIRECTOR, TERRORIST SCREENING CENTER,
BEFORE THE SENATE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS

PASSPORT INFORMATION SHARING WITH DEPARTMENT OF STATE

June 29, 2005

Good morning Chairman Collins, Ranking Member Lieberman, and members of the Committee. Thank you for the opportunity to discuss the mission and objectives of the Terrorist Screening Center (TSC) as they relate to information sharing with the Department of State (DOS).

Homeland Security Presidential Directive 6 (HSPD-6), issued on September 16, 2003, ordered the creation of the TSC, directing its operations to begin on December 1, 2003. The TSC was created to consolidate the United States Government's approach to screening for known and suspected terrorists and to provide for the appropriate and lawful use of terrorist information in this process. The TSC ensures that government investigators, screeners, federal agents, and state and local law enforcement officers have ready access to the most thorough, accurate and current information they need in order to respond quickly when a known or suspected terrorist is encountered here in the United States (US), at our borders and at our embassies.

Today, I will tell you about our daily operations as they relate to information sharing with the US DOS and specifics about our new role in their passport fraud detection program.

TSC Operations

The TSC is one of the most unique entities ever conceived or implemented to support terrorist screening and law enforcement operations. It envelops a wide range of expertise borne from a combined onsite representation of the Department of Justice (DOJ), Department of Homeland Security (DHS), the Department of Defense (DoD) and the Department of State (DOS). TSC has consolidated terrorist identities, domestic and international, in one database that is accessible to any federal, state, local, tribal or territorial law enforcement officer, as well as some foreign governments with whom the United States (US) has information sharing agreements. The TSC allows consolidated and coordinated terrorist screening at US Embassies, at the land and air borders of the US, through routine law enforcement encounters domestically, and by other countries with whom we have agreements. The TSC has created a bridge between the intelligence community (IC) and the law enforcement community to facilitate real time information sharing based on daily terrorist encounters. The TSC also has enabled real time information sharing that alerts the DoD to emerging and potential threats to the US from terrorists who are using commercial air carriers.

Since December 1, 2003, TSC has been providing key resources for screeners and law enforcement personnel. These include: (1) a single coordination point for terrorist screening data; (2) a 24/7 call center for encounter identification assistance; (3) access to a coordinated law enforcement response; (4) a formal process for tracking encounters; (5) feedback to the appropriate entities; and (6) a process to address misidentification issues.

The TSC has consolidated the names of all known or suspected terrorists within the Terrorist Screening Database (TSDB). The TSDB is fed from two primary sources: international terrorist (IT) information from the National Counterterrorism Center (NCTC) and domestic terrorist (DT) information from the Federal Bureau of Investigation (FBI). The TSDB has the names of all known and suspected terrorists in the twelve databases described in the April 2003 GAO report entitled, "Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing." The twelve databases that are currently incorporated into TSC are:

1 Consular Lookout and Support System (CLASS) – DOS
2. TIDE – National Counterterrorism Center
3. Interagency Border Inspection System (IBIS) – Department of Homeland Security 4. No-Fly – Department of Homeland Security
5. Selectee - Department of Homeland Security
6. National Automated Immigration Lookout System (NAILS) - Department of Homeland Security migrated to Treasury Enforcement Communication System (TECS)
7. Warrant Information - Department of Justice
8. Violent Gang and Terrorist Organization File (VGTOF) - Department of Justice
9. Interpol Terrorism Watch List - Department of Justice
10. Air Force Top Ten Fugitive List - Department of Defense
11. Automated Biometric Identification System – Department of Homeland Security
12. Integrated Automated Fingerprint Identification System – Department of Justice

The key to the success of the TSC's mission was to ensure information housed at the TSC was available to its customers, including the DOS. The TSC has partnered onsite with DOS since HSPD-6 was issued and established four fundamental forms of collaborative processes including: (1) Visa Security Advisory Opinion review; (2) Visa revocation review; (3) nominations to CLASS used by visa consular officers; and (4) implementing screening agreements with certain foreign governments.

DOS consular officers are our first line of defense in keeping known and suspected terrorists out of the US by denying visas to these individuals. The TSC works hand-in-hand with the Bureau of Consular Affairs on these issues. In this regard, DOS assignees at the TSC are continuing the work of reviewing visa applications against the TSDB, a

process handled through the generation of Security Advisory Opinions. Since December 1, 2003, when the TSC began operations, DOS assignees and their staff at the TSC have reviewed over 138,000 Security Advisory Opinion requests to determine if the visa applicants were possible matches with individuals in the TSDB. For example, in December 2004, an individual with links to a terrorist organization applied for a visa at a US consulate. In this case, consular officials denied the visa based on the TSC's analysis that the individual was a match to a known or suspected terrorist in the TSDB. On a separate occasion, the same process applied to a senior member of a terrorist organization based overseas. His visa was also denied.

New identities entered in the TSDB are checked against the Consular Affairs Consolidated Consular Database (CCD) to determine if those new entries had been issued visas before the derogatory information surfaced. The TSC has alerted the DOS of the need to review about 850 cases for possible visa revocation.

DOS specialists assigned to the TSC play an important role in the TSDB nominations process. The specialists ensure individuals nominated for inclusion in the TSDB are thoroughly reviewed. Additionally, the specialists ensure data is securely exported to the Consular Lookout and Support System (CLASS). CLASS is used by DOS consular officers at embassies and consulates for visa adjudication.

The DOS and TSC work together to enhance foreign government cooperation and participation in terrorist screening information agreements. The US has agreements in place with Australia and Canada for the purpose of sharing terrorist screening information to protect the US against terrorist attack. On April 19, 2005, the President formally approved the HSPD-6 report that designated the TSC as an implementing partner for any foreign sharing agreement that is negotiated by the DOS.

The screening of US citizen passport applications, a highlight of a May 2005 GAO report entitled "Improvements Needed to Strengthen US Passport Fraud Detection Efforts," is a collaborative initiative that began in late January 2005 when it was formally proposed by the DOS to the TSC. DOS and TSC immediately began discussions in early February 2005 to establish a screening agreement that aims to ensure the relevant federal agencies are aware when a US Person listed in the TSDB applies for a new, renewed, or amended US passport. A Memorandum of Understanding (MOU) between DOS and TSC to govern this arrangement is close to finalization. The TSC looks forward to continued cooperation with the DOS in this project, one in the myriad of other collaborative efforts the TSC has entered into with the DOS since HSPD-6 was issued.

Conclusion

Since HSPD-6 was issued on September 16, 2003, the TSC and the DOS have been partnering to protect our nation's security through the robust sharing of terrorist information. The TSC has provided support to those functions identified by the DOS as priorities, and will continue to share information with the DOS as mandated by HSPD-6. This close and continuing cooperation contributes to nationwide efforts to keep terrorists out of the US and locate those who may already be in the country. I would be happy to answer your questions.

The TSC thanks the Committee for the opportunity to provide clarity to this matter and looks forward to continued work with the Committee in the TSC's efforts to consolidate the Government's approach to terrorism screening.

STATEMENT OF THOMAS E. BUSH III
ASSISTANT DIRECTOR
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION
BEFORE THE SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

PASSPORT INFORMATION SHARING WITH DEPARTMENT OF STATE

June 29, 2005

Greetings Madam Chairwoman, and members of the Committee. I am Thomas E. Bush, III, Assistant Director of the FBI's Criminal Justice Information Services Division, otherwise known as CJIS. Thank you for the opportunity to appear before you and to provide testimony about the National Crime Information Center.

First, let me provide a brief overview of the CJIS Division. CJIS was created in February 1992 to serve as the focal point and central repository for criminal justice information services within the FBI. CJIS is responsible for five services to law enforcement: Fingerprint Identification, Uniform Crime Reporting, National Crime Information Center, National Instant Criminal Background Check System, and Law Enforcement Online. CJIS is the largest Division within the FBI, employing a workforce of 2,382 individuals, with nearly 200 other FBI employees stationed at the Clarksburg, West Virginia, facility in support of CJIS and other FBI operations and programs.

The National Crime Information Center, more commonly known as NCIC, is a computerized database of documented criminal justice information available to virtually every law enforcement agency nationwide, 24 hours a day, 365 days a year. NCIC became operational January 27, 1967, with the mission of assisting law enforcement in apprehending fugitives and locating stolen property. This mission has been expanded over the last thirty-eight years to include locating missing persons and further protecting law enforcement personnel and the public. Since its inception, NCIC has been a highly effective tool for information sharing with local, state, tribal, and federal entities. The FBI provides a host-computer and telecommunication network to

the control terminal agency in each of the 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, Guam, and Canada, as well as federal criminal justice agencies. Those jurisdictions, in turn, operate their own computer systems, providing NCIC access to virtually all local criminal justice agencies in the United States. Through this cooperative network, law enforcement and other criminal justice agencies across the country have direct on-line access to more than 50 million records.

NCIC has operated under a shared management concept between the FBI and state and federal criminal justice users. General policy concerning the philosophy, concept, and operational principles of the NCIC System is based upon the recommendations of the CJIS Advisory Policy Board (APB) to the Director of the FBI. The APB is comprised of top administrators from local, state, and federal criminal justice agencies throughout the United States. Through the APB, its Subcommittee and Working Group input, changes in current applications, the addition of new files, and new procedures are coordinated with all NCIC participants.

The NCIC database currently consists of eighteen files. The seven property files contain records of Stolen Articles, Boats, Guns, License Plates, Parts, Securities, and Vehicles. The eleven person files are the Identity Theft, Supervised Release, Convicted Sexual Offender Registry, Foreign Fugitive, Immigration Violator, Missing Person, Protection Order, Unidentified Person, U.S. Secret Service, Violent Gang and Terrorist Organization, and Wanted Person Files. The Interstate Identification Index, which contains automated criminal history record information, is also accessible through the NCIC network.

During NCIC's first year of operation, two million transactions were processed. In May 2005, NCIC processed an average of 4,618,321 transactions per day with an average response time less than 0.06 seconds. On May 27, 2005, NCIC processed a record 5,255,363 transactions. The FBI's CJIS Division continuously monitors the NCIC System and makes system upgrades to provide quality service.

Now, I will outline some of the NCIC files and features that assist in immigration and border security. The Foreign Fugitive File, established July 1, 1987, contains information on persons wanted in connection with offenses committed outside the United States. There are two types of records in the Foreign Fugitive File: Canadian records and International Criminal Police Organization (otherwise known as INTERPOL) records. Canadian records contain information on persons wanted for violations of the criminal code of Canada based upon Canada-wide warrants. INTERPOL records contain information on persons wanted by authorities in other countries. The INTERPOL National Central Bureau of any country may issue a wanted flyer, known as a red notice, for a fugitive wanted within its respective country. The red notice requests the arrest of the fugitive with the intention that extradition will occur. Upon receipt of a red notice, the United States INTERPOL National Central Bureau reviews the information and enters an NCIC Foreign Fugitive File record if the following conditions are met: 1) the wanting country has an outstanding arrest warrant that charges a crime which would be a felony if committed in the United States; and 2) the wanting country is a signatory to an extradition treaty/convention with the United States. On June 1st of this year, there were 1,128 records in the Foreign Fugitive File.

The Immigration Violator File was established on August 25, 2003. In 1996, NCIC implemented the Deported Felon File; today, this is a category of records within the Immigration Violator File. The Immigration Violator File includes two additional categories of records; Absconders and the National Security Entry/Exit Registration System (NSEERS). The Deported Felon Category contains records for previously deported felons convicted and deported for drug trafficking, firearms trafficking, or serious violent crimes. The Absconder Category contains records for individuals with an outstanding administrative warrant of removal from the United States who have unlawfully remained in the United States. The NSEERS Category contains records for individuals whom Department of Homeland Security, Immigration and

Customs Enforcement has determined have violated the requirements of the NSEERS. An Immigration Violator File hit response includes guidance to the local law enforcement agency on handling the hit. The Department of Homeland Security, Immigration and Customs Enforcement, is the only agency authorized to enter and maintain the Immigration Violator File records. On June 1st of this year, there were 163,342 records in the NCIC Immigration Violator File.

The Violent Gang and Terrorist Organization File or "VGTOF" was implemented in December 1994. This file is designed to provide identifying information about violent criminal gang and terrorist organization members to protect the law enforcement community and the public. For our purposes today, I will limit my statement to the terrorist records within VGTOF. During security preparations for the 2002 Winter Olympic Games in Salt Lake City, Utah, the FBI determined that it would be advisable to have individuals of FBI domestic or international terrorism investigative interest included in VGTOF. Traditionally, NCIC person records serve the needs of the criminal justice community and are supported by the judicial process. Most typically, a warrant is on file. However, with the creation of VGTOF, that philosophy was expanded to support law enforcement investigative and information needs related to terrorism. The terrorist records, in particular, support national security and homeland security. Based on the positive results during the Olympics, the FBI has continued to make this terrorism information available to the criminal justice community and has enhanced VGTOF to better support these records. The Terrorist Screening Center (TSC) became operational on December 1, 2003, and the FBI CJIS Division has modified the NCIC VGTOF to support TSC's mission. The VGTOF is the means to make the terrorist screening information available to the law enforcement community nationwide. When an officer hits on a VGTOF terrorist record, he is instructed to contact TSC for additional information on the subject.

The Department of State (DOS) Bureau of Diplomatic Security is a fully authorized NCIC user when conducting criminal investigations. Additionally, the FBI has provided the DOS Bureau of Consular Affairs with extracts of the NCIC Wanted Person, Immigration Violator, Foreign Fugitive Files, VGTOF, and the Interstate Identification Index, on a daily and weekly basis, for inclusion in its Consular Lookout and Support System (CLASS) as required by Section 403 of the USA PATRIOT Act in support of the visa adjudication process. The Department of State uses the information to ascertain whether visa applicants have records indexed in NCIC which might preclude the issuance of a visa.

In late April of 2005, CJIS received a request from DOS Passport Services for an extract of the FBI fugitives contained in the NCIC system. Our immediate response was that FBI fugitives in NCIC represent only a fraction of the more than one million felony and serious misdemeanor wanted person records entered into NCIC. We have requested that DOS Passport Services work with the FBI toward the ultimate goal of system interoperability and direct NCIC access for passport screening. As an interim step toward this goal, we have agreed to provide the requested extracts.

The Department of Homeland Security components are indisputably NCIC's largest customer and have been using the system for three decades. NCIC is a valuable tool for immigration and border security as is clearly demonstrated by the fact that one third of NCIC transactions are performed by the Department of Homeland Security, Bureau of Customs and Border Protection. These transactions include inquiries on individuals and property entering and exiting the United States and encompass airline passenger manifests.

Over 17,000 law enforcement agencies query NCIC in the performance of their daily activities, to include routine patrols. The inclusion of the Department of Homeland Security component information in NCIC makes that information instantly available to over 700,000 law enforcement officers nationwide and significantly

multiplies the enforcement resources brought to bear on immigration and border security issues.

In closing, I would like to thank you for allowing me the opportunity to explain the use of NCIC for immigration and border security. I will now answer any questions you might have.

LOCAL 1998

National Federation of Federal Employees
International Association of Machinists & Aerospace Workers, AFL-CIO

July 14, 2005

To: Sen. Susan Collins, Chair – Senate Homeland Security & Governmental Affairs Committee

Re: Union's Views on Hearing & Report on Passport System Vulnerabilities

Sen. Collins:

I am respectfully requesting that this statement be included in the official record of the June 29th hearing that the Senate Homeland Security & Governmental Affairs Committee held, titled "Vulnerabilities in the U.S. Passport System Can Be Exploited by Criminals and Terrorists". I am writing to you in my capacity as the Union President of NFFE Local 1998, the exclusive representative of the Passport Services bargaining unit employees.

The GAO report and your hearing addressed seven general topics: 1) problems with the CLASS namecheck system; 2) unreasonable adjudication performance standards; 3) the lack of a centralized online fraud prevention library; 4) problems with workload transfer applications; 5) insufficient fraud prevention staffing (the elimination of the Assistant Fraud Program Manager position); 6) insufficient anti-fraud training for Passport Specialists; and 7) insufficient fraud prevention oversight of Acceptance Agents.

By far the single most frequent, most vocal, and most serious complaint our union has heard from the employees is the concern our Passport Specialists have with vulnerabilities affecting the integrity of the passport issuance process. Our union repeatedly conveyed these concerns to management officials and attempted to address this issue through negotiations, partnership meetings, grievances, and unfair labor practice charges. On those occasions when we have used these traditional channels to solve or contest more typical employee complaints or concerns, but were unsuccessful, we accepted that verdict and moved on. This issue is different: this affects national security. We therefore reluctantly decided to take the unprecedented step (in the history of our local) of asking Congress for help. Employees in most of our offices participated in our letter-writing campaign, and we received a great deal of support from the IAMAW, NFFE, and our families and friends. We are thankful for all of the helpful and interested responses we received from many members of Congress.

On behalf of the bargaining unit employees that our union represents, thank you for your effort, time, and energy on this important subject. We also greatly appreciate the interest and intellect of your staff and the attention they gave to our concerns. We concur with your statement that the GAO performed an "excellent investigation" and our compliments to their professional staff.

I believe that the newly announced link between the Department of State (DOS) and the Terror Screening Center (TSC) and the pending agreement between DOS and the Federal Bureau of Investigation (FBI) that partly solves the problems with CLASS are the direct result of the light shined on this subject by your committee and by the GAO. I also believe that solutions that are emerging to some of the other issues, such as the creation of centralized online fraud prevention

library, are also happening because of the committee hearing and the GAO's report. These improvements would not be taking place without Congressional oversight.

I would like to emphasize that it is my firm belief that all of the managers, supervisors, and employees of Passport Services are united in their desire to maintain and enhance the integrity of the passport issuance process. We share a common goal. No one wants to issue a passport to a terrorist or a criminal. Where the union and the employees disagree with management is in our analysis of how serious is the threat, how vulnerable is our system, and in what steps we should take to deter and detect passport fraud. Many of the senior management officials have never adjudicated a passport application, and none have done so on a routine basis in the last few years. The employees that this union represents have adjudicated over 50 million passport applications in the last decade and are being called upon to adjudicate another 50 million in the next four years. We believe that our collective wisdom should inform the decisions that are made on this vital issue.

The GAO's report drew firm, critical conclusions on six of the seven topics investigated. On the remaining topic – the adjudication performance standards – while the Department of State's methodology was criticized, no conclusions were drawn in the GAO's report since constantly changing work processes made a verdict "premature". We continue to have very serious concerns about this subject. In a recently conducted survey, 96% of Passport Specialists reported that the current standards do not afford them enough time to diligently adjudicate and detect passport fraud, and 93% reported that employees are forced to take shortcuts in order to meet the standards. We would prefer to work with management to address this problem, but if that does not transpire then we hope that this will continue to draw the attention of your committee and the GAO.

We also believe we need fundamental changes in our work culture. First, rather than accepting the status quo, we need more imagination to identify ways to improve ourselves along with the willingness to take action. Second, the mission of the Agency would be better accomplished if management worked with the union and heeded the concerns of the employees. We need to place more emphasis on fraud detection in promotions, evaluations, and awards. Management should seek out input and feedback from the union and the employees on issues that affect how the work is performed – for example, on the issue of the fraud library, it should be user-friendly, incorporate ideas from employees, be regularly updated, and we should received training on how to use it. Third, employees should be able to express their concerns to the Congress, the OIG, and to the GAO without fear of retaliation: we should "Put loyalty to the highest moral principles and to country above loyalty to Government persons, party, or department" (the U.S. Government Code of Ethics). Fourth, there needs to be some clearly identifiable office that is in charge of passport fraud and vulnerability issues, to whom some of these concerns can be addressed.

Thank You,

Colin Patrick Walle
Union President
IAMAW NFFE FD1 Local 1998

Attached: specific responses to the testimony and conclusions on many of the topics addressed in the HSGAC hearing and the GAO report

LOCAL 1998

National Federation of Federal Employees
International Association of Machinists & Aerospace Workers, AFL-CIO

Union's Views on Hearing & Report on Passport System Vulnerabilities

General Observations

Less than 5% is not a success: According to the DOS, 50,000 fugitives were already listed in CLASS. But, since the FBI has over 1,200,000 names of fugitives in their database, that 50,000 figure represents less than 5% of the fugitives wanted by law enforcement entities, meaning more than 95% of them would be able to obtain a passport.

99% is not good enough: 99% of the people who fly on airplanes, immigrate to the U.S., or enter federal buildings are not terrorists or criminals, yet that does not mean there are no vulnerabilities with immigration, airplanes, and metal detectors. Most U.S. passports are issued to bona fide applicants – because most of our applicants are not *attempting* passport fraud. A DOS "validation study" uncovered 3 "potentially serious frauds" out of 10,000 applications: the GAO pointed out that extrapolates into 3000 missed frauds out of 10 million applications. Diplomatic Security opened 1722 fraud investigations in FY2004, so that figure of 3000 is a very significant number.

"A rising tide lifts all boats": The number of passport applications went up 22% from FY2003 to FY2004 and is going up about 14% from FY2004 to FY2005. While there is not an exact correlation between bona fide and fraudulent applications, if the workload goes up 20% but there is a 10% increase in fraud detections, that is not an improvement.

Apples vs. Apples & Oranges: For sensitive reasons we cannot go into detail here, but it is important to understand that for many years fraud detection statistics counted "apples" only, and now those same "apples" are being counted but a new category of "oranges" has been added. It is important to compare "apples to apples" when measuring any changes.

Lets not wait for disaster to strike

There have been many instances of important changes only happening after something terrible happens. According to many printed and online references, the Canadian Passport authority enacted stricter application requirements in 1969 after they found that James Earl Ray, the assassin of U.S. civil rights leader Rev. Martin Luther King Jr., had fraudulently obtained a Canadian passport. In 2004, DOS made it a requirement that all minors personally appear for their passport applications, which was done after many passports were issued in error to fraudulent persons attempt to smuggle children into the U.S. or to commit identity theft (e.g., when 7 Chicago-area residents were indicted last year for allegedly fraudulently obtaining 300 – 500 passports to smuggle children into the U.S. The shrinking number of visa applicants receiving face-to-face interviews by the Department of State (including the infamous "Visa Express" program in Saudi Arabia) went on for some time even though it received criticism. Only after September 11th was this policy reconsidered. It is all too possible, some would say plausible, that a passport we have issued or will issue will play some part in a future terrible event. The GAO report is the "writing on the wall": there are sufficient danger signs that should prompt actions now, before disaster strikes.

Problems with the CLASS namecheck system

Are terrorists attempting to obtain U.S. passports?

At the June 29th hearing, Sen. Collins asked if "terrorists are trying to get their hands on U.S. passports?" The answer is "yes". For example, at a DOS press briefing on June 11, 2002, Spokesman Richard Boucher outlined how Jose Padilla, who is currently in custody and is alleged to be a member of Al-Qaeda and an alleged "dirty bomb" plotter, was apprehended as a result of an investigation generated by his passport application at the U.S. Consulate General in Karachi, Pakistan. At a DOS press briefing on November 13, 1996, Acting Spokseman Glyn Davies mentioned the arrest of Marwan Abid Adam Kadi aka Ibrahim Mahmood Awethe on passport fraud charges in Paraguay and his extradition to the U.S., and he is asked if there is a connection to a travel warning about the election day in Paraguay but cannot comment. According to media reports, Laura Whitehorn, allegedly part of the domestic terrorist Weather Underground and May 19th Communist groups, was convicted of passport fraud charges in the 1980's. Also according to media reports, James Kilgore, a former member of the domestic terrorist Symbionese Liberation Army group, pled guilt to passport fraud and explosive charges for acts committed in 1975.

According to the 1976 DOS book "The United States Passport: Past, Present, Future", passport fraud has been "perpetrated in the United States by criminals, fugitives from justice ... [and] terrorists ...". That book related that the penalties for passport fraud were increased during World War I when the British government found German espionage agents using altered U.S. passports. There has been a longstanding concern that terrorists or dangerous criminals may obtain passports.

Obviously, legitimate travelers outnumber fraudulent applicants for U.S. passports. Also, criminals and fugitives outnumber terrorists in the ranks of those who are committing passport fraud. Yet, still there is a real threat that terrorists have attempted or will attempt to obtain U.S. passports. Even more worrisome is the possibility that some already have. This is where the example of James Kilgore is pertinent. From 1975 to 2003 – a span of 28 years – the DOS was not aware that we had issued a passport to a member of the domestic terrorist group Symbionese Liberation Army. Did we issue any other passports to dangerous criminals or terrorists in the last quarter-century, the last decade, the last year, or the last month, that we won't become aware of until years from now?

Vulnerabilities existed and were known for many years

A major vulnerability in the passport system addressed by the GAO and the HSGAC, which garnered widespread media coverage, was the problems with the CLASS database and the fact that terrorists and wanted criminals were not listed in that database and could therefore successfully apply for a U.S. passport in their own true identity. As a result of the HSGAC hearing and the work done by the GAO, the DOS, FBI, and TSC are taking steps to make connections that should hopefully solve this problem in the future. We believe that the importance of checking our applications against these databases outweighs concerns that they will "clog" our system.

According to the GAO report, "State officials told [the GAO] they had not initiated efforts to improve information sharing with the FBI on passport-related matters until the summer of 2004 because they had previously been under the impression that the U.S. Marshal's Service was already sending to CLASS the names of all fugitives wanted by federal law enforcement authorities".

However, DOS managers, supervisors, and employees have been aware for many years (long before September 11th) that many dangerous criminals were not listed in the CLASS database. Many employees and managers have seen cases where a person was not listed in CLASS but turned out to be wanted after Diplomatic Security, while investigating a fraud referral, uncovered this fact after checking with NCIC (while the FBI's CJIS Assistant Director Bush stated that Diplomatic Security "is a fully authorized NCIC user", they could only run the names of those referred to them). Special Agent Michael Johnson cited an example of this problem in his testimony.

According to the DOS, half of the "nearly 50,000 names of fugitives or other individuals of interest to law enforcement" were "entered individually as a result of our outreach efforts" – for example, at conferences or meetings where law enforcement personnel were scheduled to attend, brochures and contact information would be distributed (part of "our outreach efforts"). This was done so that the DOS could educate the officers or agents on the fact that fugitives were not automatically listed in CLASS and that they therefore had to make an effort to have them listed.

In December 2003 the Union brought concerns to Management about terrorists and other dangerous criminals not being listed in CLASS. One Union representative cited two examples from her Passport Agency (one applicant had al-Qaeda links and a second turned out to be on a terrorist watch list but had already received nine passports – neither were in CLASS). The response that the Union received was that anyone with a warrant should have been entered into CLASS by law enforcement and they would pass on our concerns.

Employees then checked the names of the FBI's Ten Most Wanted list against CLASS to see if this vulnerability had been addressed: the results were that some were not listed. This information was reported to Congressional staff, to the GAO, and to the DOS's OIG. The GAO then investigated this further, and the result of their test of 67 fugitives' names was that 37 were not listed in CLASS.

Additional actions and enhancements should be considered

The GAO report noted that applications are checked against the DOS's own MIV database to see if a passport was issued in the last 10 years. Originally, that check was done only against the last 3 years. There have been instances where multiple people applied for passports in the same identity more than 10 years apart and they would not have been caught absent fraud indicators on the current application (e.g., four individuals obtained five passports in the same identity). We suggest that MIV be expanded to check all previous passport records.

The pending connection between CLASS and the TSC and FBI databases will have a positive effect in ensuring that future passport applications are properly checked. While we are not aware of any software that could automatically check the names of the 1.2 million fugitives against CLASS (a much larger version of the GAO's test), some consideration should be given to checking the most dangerous fugitives, as that may provide leads for law enforcement.

The GAO report mentioned that the link between DOS and the SSA would not include death records, yet these records are commercially available for a relatively cheap price. CLASS should be upgraded so that we will be able to know if the applicant is using a deceased identity.

Information sharing should go both ways. The DOS has lists of missing blank citizenship documents (e.g., birth certificates) and other information that may be useful to other agencies.

Unreasonable adjudication performance standards

"Increased pressure on examiners to focus on production numbers"

The GAO report found that because the DOS "adjusted the impact of production on examiners' evaluations, the production standards implemented in 2004 placed increased pressure on examiners to focus on production numbers". We concur with this assessment, and we repeat once again: we simply do not have sufficient time to diligently adjudicate passport applications. What that means is that by focusing on achieving the quota we don't have time to properly scrutinize the applications and the evidence submitted for fraud indicators. We need more time. At the pace we are working, it is all too easy for a person attempting to commit passport fraud to be successful.

According to the GAO, one specialist "noted that if she failed to check any fraud indicators at all and granted a passport to every applicant, she would be right more than 99 percent of the time." That is because most of our applicants are not choosing to commit passport fraud, not because we are doing an outstanding job in detecting those who are. One problem in any analysis of frauds issued in error is that generally our knowledge of them only comes after another government agency catches them after the fact, so we have no idea how many have been issued in error that have not been caught by others. However, in the view of many experienced Passport Specialists, the majority of the numerous frauds issued in error that we are aware of should have been detected during the adjudication process. Considering this, it would unfortunately be all too easy to imagine a presumably more sophisticated attempt by a terrorist to likely succeed since Passport Specialists are simply forced to work too quickly to be able to detect many fraud attempts.

The production standards should be lowered as soon as possible. The quotas should be determined by a fair and accurate study, developed and monitored an independent outside authority or by both Management and the Union. There should be consideration for eliminating the quotas completely. We understand that, after September 11th, immigration inspectors had their 30-second average quota eliminated. Since there are pressures for more travelers to come to the DOS to obtain passports rather than submitting one of thousands of versions of citizenship/identity documents at the border, then this idea seems all the more reasonable. In addition, many offices previously did not have quotas for expedite applications, yet the three working day processing commitment was met.

Management responds to union and examiner concerns

The GAO report states, "in response to union and examiner concerns, State eased the production standards during 2004 and made a number of other modifications and compromises". It would have been helpful if we had been told at that time that this was done in response to our concerns.

The affect of the current performance standards on fraud detection

The GAO report states that because the DOS's "changes to the production standards continued throughout 2004, the standards' net effect on fraud detection efforts remains unclear". We hope that Management will listen to our concerns and work with the Union, but if not, then we hope that this issue continues to draw the attention of your committee and the GAO. To find out how the standards are measuring up right now, we conducted a survey of Passport Specialists on 6 questions. To sum up the results of the survey:

- We do not have enough time do diligently adjudicate and detect passport fraud
- We have to take shortcuts in order to make the quota
- In our jobs, "*Quantity* is Job 1"
- We are concerned that we will issue a passport in error to a terrorist or criminal
- We need more anti-fraud resources and training, but we also need time to use them

Questions	Answers
1. Do the numerical performance standards provide you with sufficient time to diligently adjudicate passport applications and detect passport fraud?	**No - 96%** **Yes - 4%** (No: 131, Yes: 6, Don't know/NR: 2)
2. Do you have to take shortcuts to make your quota? Shortcuts include: A) failing to consistently compare info (name, gender, address, etc.) on evidence vs. application vs. screen on **all** applications; B) rushing through the process so that you are not properly scrutinizing the application for fraud or errors; C) avoiding complex cases/batches ("cherry-picking"); and D) working through lunches, breaks, and the allotted one hour of reading/preparatory time. What percentage of Passport Specialists do you believe have to take shortcuts to make the quota?	**Yes - 93%** **No - 7%** (Yes: 126, No: 3, No but others do: 6, Don't know/NR: 4)
3. Do you feel the emphasis in the job (retention, appraisals, awards, promotions) is more on quantity or quality, or is there a good balance?	**Quantity - 94%** **Balance - 6%** **Quality - 0%** (Quantity: 122, Balance: 8, Don't know/NR: 9)
4. How concerned are you that *you* will issue a passport to a criminal or terrorist? How concerned are you that a *coworker* will?	**Concerned – 94%** **Not Very Concerned – 6%** (Very concerned, concerned, & somewhat concerned: 122, Not very concerned: 5, Not since supervisors aren't: 1, Not since not enough resources: 1, Not but confident others will: 1, NR: 9)
5. Are sufficient anti-fraud resources (intranet and hard copy) and anti-fraud training provided to employees?	**No – 54%** **Yes – 27%** **Not enough time – 19%** (No: 71, Yes: 35, Not enough time: 26, NR: 7)
6. If you here the claim that "nearly every specialist is making the numbers, so that proves that the standards are just fine and there is no reason to reduce them", how would you respond?	**Disagree – 98%** **Agree – 2%** (Disagree: 129, Agree: 3, Unclear/NR: 7)

The survey was emailed to all bargaining unit employees, approximately 73% of which are Passport Specialists. 139 Specialists responded between June 27th and July 8th to the survey out of approximately 336 who received the survey. This 41% response rate is the highest response rate to any survey the Union has distributed in at least the last 7 years. (NR = No Response or unclear response)

Vulnerabilities in the adjudication process

When asked during the June 29th hearings how difficult it would be for a terrorist to obtain a passport, Special Agent Johnson replied that it would be relatively easy. His answer was based upon the ease and speed with which an identity thief can obtain citizenship documentation, either legitimate or counterfeit. The unspoken implication was that the Passport Specialists are too often unable to detect these cases during the application review process.

Although the DOS charges $157 for an expedited adult application, the typical application will receive only about 2 minutes of time being adjudicated. A Passport Specialist is supposed to do the following tasks when adjudicating applications:

1) Obtain the batches of applications

2) Log the batch numbers into the computer
3) Unstaple the applications from the attached evidence
4) Separate the 2 pages of the application from each other (when they are still attached)
5) Scan the barcode of the applications into the computer, one at a time while adjudicating
6) Compare the information on the evidence against the information on the application against the information on the screen
7) Make corrections as necessary
8) Make notations on the application – usually about a dozen
9) Handle any CLASS information that appears on the screen (page 8 of the GAO report): CLASS, CLASP, PLOTS, MIV/IP, SSA, and PIERS.
10) Re-run CLASS, as needed
11) Scrutinize the evidence for fraud indicators
12) Scrutinize the application for fraud indicators
13) Utilize information from the screen to discern if fraud is being committed
14) Utilize printed and online anti-fraud resources
15) Adjudicate the application to determine citizenship, identity, and other requirements have been fulfilled – some of these tasks are:
    a. Ensuring proper fees paid,
    b. Ensure proper photos submitted
    c. Ensure proper execution procedures followed and that application was submitted at an authorized acceptance facility
    d. Adjudicate complex citizenship cases, which can take between 10 minutes up to even a few hours each (no time is subtracted for these cases) – the DOS previously charged applicants an additional $100 fee for some types of these cases, since they took so much more time and resources
    e. For minor children, ensure parental approval
16) If insufficient evidence or incorrect documentation/fees submitted, remove the application from the batch and take additional steps (e.g., selecting letter or calling the applicant)
17) Staple the 2 pages of the application back together, along with any affidavits or attachments
18) Ensure that the delivery type is correct and enter Express Mail tracking code when needed
19) Approve the application on the screen
20) Sign the application
21) Affix name-stamp to application
22) Put the evidence into an envelope (folding when necessary)
23) Paper-clip the envelope and the second photo to the application
24) Move the batch to the next step when all applications completed

Passport Specialists have to take shortcuts in order to make their quotas, but they cannot choose to skip "mechanical"/"clerical" steps such as unstapling/stapling, scanning, stamping, making notations, signing, changing delivery type, or stuffing envelopes. If a Specialist chose to skip one of these steps on every application, he/she would have potentially a 100% error rate, 100 times higher than the 1% allowed. No Specialist intentionally fails to overlook fraud indicators, but most Specialists report that they believe that by rushing through the work so quickly, they have and will make serious mistakes. Since most of our applicants are bona fide citizens and are not fugitives, then as the employee cited by the GAO stated, "if she failed to check any fraud indicators at all and granted a passport to every applicant, she would be right more than 99 percent of the time." The DOS validation study can count how many times a Specialist failed to make a notation or staple an application, but they cannot measure how much or how little time was spent scrutinizing the

applications, the evidence, and the computer tools for fraud indicators. The cost/benefit analysis of our priorities needs to shift: as one respondent to our survey noted, if we correctly issued passports to 199 passengers on an airplane but also issued 1 passport in error to a terrorist on that same flight, we would have failed the American people.

This is a key point to keep in mind as additional tools – such as connections to the TSC and FBI, and the creation of an online fraud library – are implemented. Since most fraud applications are detected not by looking "behind the paper" but rather by looking *at* the paper (application and evidence), any additional assignment – no matter how worthy – takes time away from the level of scrutiny necessary to detect passport fraud. The Union has consistently and repeatedly stated that we support the inclusion of the technological improvements and additional anti-fraud tools; we have simply made the point that we need enough time to use these tools. For example, there have been a few cases where an applicant who was in CLASS for passport fraud was issued in error despite that fact, so time pressures can even undermine any improvements made to the namecheck system. If the other 95% of the fugitives were added to CLASS and we checked all of our passport records instead of just the last 10 years, those would be great improvements – but they will also take more time (hence the DOS's worry that this will "clog" our system).

The current performance standards are just slightly lower on average than they were 5 years ago, but it is important to understand that a quota of 24 per hour does not mean that we have more time for fraud detection than a quota of 25 per hour for the following reasons:

- Previously the quotas were not as strictly enforced, or were mixed in with other job elements, so that an employee with a 25 per hour quota but who produced 22 could still be rated Fully Successful or even higher.
- Numerous additional duties have been added. The task of checking CLASS, MIV, etc. was added when we converted to the Photodigitized passport process. Previously, applications would be adjudicated without Specialists checking this information (possible matches were removed at a later stage to be handled by another assignment that had not quota).
- New laws and policies. The Child Citizenship Act of 2000 created a new way to acquire U.S. citizenship and changed requirements for others – these cases are time-consuming. The Two-Parent Consent rule requires us to perform many tasks that were not performed before.
- The easier applications are gone. In many offices, the applications adjudicated at the counter would be "run through" by other Specialists at their desks trying to achieve the quota. Since most of the tasks for these applications (including approval) were already done, they added to the total output by the employee. The appointment system drastically cut down on the numbers of these applications and new procedures require employees who are not assigned to meet the quota to handle these cases. This mirrors what happened since the mid-1990's when all of the renewal applications began to be sent to one of the megacenters, leaving employees without the easier applications but with the same quota.
- Design changes make it harder to adjudicate. The Union has received over 80 emails on the subject of the new 2-page application, many from Union officers who have surveyed the employees in their offices (so some of those emails represent the views of a dozen or a score of other employees). With the exception of 2 individuals who felt the new forms had no impact, every other email complained that the new forms take more time. The design of the computer screen is not user-friendly. The Union and the employees were not afforded the opportunity to give feedback on the designs for the screen and the application.

- At our offices that have the heaviest fraud workload (New York, Miami, and Los Angeles), previously the quota was based only on adjudicating the application and evidence, now they have to perform numerous steps on the computer in addition to the paper steps.

The scenario in this chart illustrates how quantity expectations trump all other considerations:

Job Element	Rating	Overall Rating	Consequences
1. Adjudication Knowledge Critical Element	Outstanding	**Unacceptable**	• Ineligible for WGI • Ineligible for promotion • Difficult to obtain another federal job • Not likely to receive award • Placed on PIP • If PIP not successful (need to raise 23 to 24), then subject to performance-based action: o Downgrade o Removal
2. Customer Service Critical Element	Outstanding		
3. Fraud Awareness Critical Element	Outstanding		
4. Security Awareness Non-Critical Element	Outstanding		
5. Production/Technical Skill Critical Element	**Unacceptable**		
Element 5 subparts:			
Legibly records documents	Outstanding		
Ensures fees are submitted/recorded	Outstanding		
Administers oath	Outstanding		
Determines priority of service	Outstanding		
Averages **24** applications/hour	**23 per hour: Unacceptable**		
Desk notational error rate less than 1%	Outstanding		
Verifies TDIS info - error rate less than 1%	Outstanding		
Accepts/adjudicates 7/hour at counter	Outstanding		
Counter notation error rate less than 1%	Outstanding		

Rating system: employees can be rated from Unacceptable to Fully Successful to Excellent to Outstanding
PIP = Performance Improvement Plan WGI = Within-Grade Increase

A All of the "carrots" and "sticks" we have are either based on quantity considerations or trumped by quantity considerations. Besides lowering the quotas, the Union believes that we need changes in the promotion, evaluation, and awards formulas that will place more emphasis on fraud detection. In addition, there is no ceiling to production level ratings, but we believe there should be some minimum amount of time spent on each application.

The 99% figure cited by the employee may be true in regard to fraud attempts, but it does not mean that 99% of applicants submit the required documentation to obtain a passport. Between 5% and 10% of applications are temporarily denied because they lack items/information that would enable approval of their passport. Unfortunately, some of the requirements in our form letters have been weakened in ways that may make identity theft easier. One way to correct this would be to involve fraud prevention staff in vetting the form letters.

Flawed methodology undermines the establishment of reasonable standards

The GAO criticized the DOS's methodology in the establishment of the nationwide standards in January 2004. The Union's main objection to the methodology is that Management is counting *what* people are producing, ignoring the fact that *how* they are producing those numbers is of grave concern. Considering that 93% of employees take shortcuts to produce that quota that means the quota is a standard that requires shortcuts to be taken. A reasonable standard would be one that did not require employees to take shortcuts and which provided sufficient time to diligently adjudicate applications and detect passport fraud.

Problems with workload transfer applications

As stated in our cover letter, the difference the Union's/employees' position and Management's position is not one of intentions or goals but rather how seriously we view the vulnerabilities. We dispute the notion that this is a "hypothetical" problem. This is a very serious, very real problem. For years there had been widespread concerns about low fraud detection rates in workload transfers but many only had anecdotes to support their worries. In 2003 the Union forwarded to HQ Management an analysis based on hundreds of thousands of workload transferred applications over a 60 month time period that showed that one office was referring applications to the fraud prevention office at 1/3 the rate of another office, from work generated by the same region. The GAO investigation confirmed that there were significant, statistically verifiable, decreases in fraud referrals as a result of workload transferred applications.

The DOS position is that "we successfully address this risk through our selection of highly skilled Fraud Program manager, by rotating our senior passport specialists through the FPM office so that they can then assist and better train their staff, and by training centrally all of our newly hired specialists." While the latter point is a good idea in order to have consistent training nationwide in terms of citizenship adjudication and procedures, the training program has little connection to solving the problems with workload transfers. Those three offices have "highly skilled" FPM's, and two of them also had highly skilled AFPM's, but their job is not to perform the initial detection of passport fraud – that is the job of the Passport Specialists.

The GAO report found that this problem extended to all of the offices receiving transfers, so that fact would invalidate the hypothetical idea that there was a problem with any one former manager in one office. Considering that the employees in those offices are dedicated public servants, why is there a problem with fraud detections in workload-transferred applications? The answers we have received from employees in those offices are that the offices are run like factories and they have huge pressures to make their quotas, that they have great difficulties in dealing with cases from all 50 states rather than a smaller region, and they do not have sufficient anti-fraud training or resources to help them.

Most of the specialists in all of our offices have complained about the lack of resources and training as well as production pressures. There appear to be two key differences between the 13 offices handling only their own work and the 3 that handle workload transfers. First, it appears that the carrots and sticks to meet or beat the quota (even on a daily basis) are even more pronounced in those offices. Second, the employees have reported to the Union the same problems with detecting fraud while dealing with such a diversity of applications that they reported to the GAO. These Specialists have to handle cases from all around the country, while over the years regional office employees develop expertise and familiarity with documents and characteristics from a much smaller area. The solutions to the other problems addressed by the GAO report would help alleviate some of the workload transfer problems: more training and resources, more time to adjudicate diligently, less pressure to achieve production standards, better connections to other databases, and additional anti-fraud staff (two FPM's each, along with additional AFPM's). Yet, the problems faced by Specialists in dealing with identity and citizenship documents from all 50 states, as well being familiar the "demographics, neighborhoods, and other local characteristics of a particular region".

Insufficient fraud prevention staffing (the elimination of the AFPM position)

We strongly disagree with Management's decision to eliminate the Assistant Fraud Program Manager (AFPM) position, which we believe was a big step backwards in the effort to prevent passport fraud. At a time when we need more permanent fraud prevention staff, Management decided to cut it by 47%. Hopefully Management will reconsider this decision.

Sen. Collins expressed "concerns about the elimination of the assistant fraud manager position and ... not enough resources are focused on fraud detection and prevention". The DOS reply:

> Let me begin with the issue of the so-called elimination of the assistant anti-fraud program managers. What we had was a situation where we had a couple of people encumbering these positions, and some other people who had been assigned to this function, basically on informal details at the passport agency level. What we were trying to do, Madam Chair, in this effort, is to make certain that the knowledge that is held by our fraud program managers really gets out onto, if you want to talk - for want of a better term, onto the passport floor.

The Union's view on this is as follows:

- There were not a "couple of people" – meaning two – encumbering these positions, but rather 14 in 12 offices, according to the GAO. The majority of offices relied on AFPM's.
- Absent the November 2003 decision to cut the permanent staff, there probably would have been 3 more AFPM's in 2 of our other offices (Charleston and Honolulu). Teams of Management officials reviewing those offices made those recommendations earlier in 2003.
- The statements "so-called elimination" and "informal details" obscure the fact that in the early 1990's there were four GS-9 AFPM's (in Miami, New York, Los Angeles, and New Orleans) who had official Position Descriptions (PD). When the GS-5/7/9 Passport Examiner position was upgraded to the GS-5/7/9/11 Passport Specialist position in 1996, the GS-11 PD Specialist PD supplanted the GS-9 AFPM PD. The former DAS and former Managing Director who pushed for the upgrade of the examiner/specialist position up to a GS-11 were concurrently responsible for the expansion of the AFPM's into more offices.
- The post-1996 AFPM's shared the same PD as the specialists, but they had their own Performance Standards and Job Elements. It is not uncommon for different jobs to be based on the same PD. Specialists at the Special Issuance Agency and the Office of Information Management & Liaison have different tasks than their counterparts in the 15 other offices.
- Prior to the elimination of the permanent AFPM's, "the knowledge that is held by our fraud program managers" was getting out "onto the passport floor" to the extent that GS-11 specialists already were rotating through to assist both the FPM and the AFPM. When the FPM was absent or otherwise unavailable, the rotating specialists would still receive expert guidance and training from the AFPM. Eliminating the AFPM's only exacerbates problems with insufficient anti-fraud training for both the staff and the rotating specialists.

At the time that the permanent AFPM's were eliminated (January 2004), there were 14 AFPM's and 16 FPM's, so Management's decision means they were cutting the permanent anti-fraud program staff by 47%. The Union's more limited research found 12 AFPM's in 10 offices (we respect the fact that the GAO's information is more accurate than ours), so considering that Boston had a position that was unfilled, up to two positions had been recommended for Charleston (CPC), and

even one position was recommended for Honolulu, then per our statistics there would have been 16 AFPM's to go with the 16 FPM's – a 50% drop in permanent anti-fraud staffing.

Furthermore, the office with the most applications (NPC – with 29%) and the office with the third most (New Orleans – 14%) each had 2 AFPM's. There were AFPM's or recommended spaces for AFPM's in the 13 offices that issued a combined 94% of passport in FY2004.

AFPM Comparison Based on Union's statistics	Did the office have a permanent AFPM?	Total Applications Issued in FY2004	% of Applications
Boston	Yes *	308,024	3.49%
Chicago	Yes	326,475	3.70%
Connecticut	No ****	127,487	1.44%
CPC	Recommended **	1,469,936	16.66%
Honolulu	Recommended **	70,962	0.80%
Houston	Yes	367,374	4.16%
Los Angeles	Yes	351,739	3.99%
Miami	Yes	350,294	3.97%
New Orleans	Yes - two	1,238,880	14.04%
New York	Yes	165,945	1.88%
NPC	Yes - two	2,574,432	29.17%
Philadelphia	Yes	358,382	4.06%
San Francisco	Yes	291,668	3.30%
Seattle	Yes	369,891	4.19%
SIA	No ***	191,197	2.17%
Washington (WN)	No ****	262,724	2.98%
Total Applications		8,825,410	

* Boston's AFPM was promoted to the FPM - no replacement was selected by the time the permanent AFPM's were eliminated
** 2003 MA/ICR's recommended one or even two AFPM's for CPC and one AFPM for Honolulu
*** SIA issues official, diplomatic, and military dependent passports and therefore has a low rate of fraud
**** We do not have copies of MA/ICR reports for Connecticut and Washington, so we do not know whether or not an AFPM position was recommended for those offices as was recommended for CPC and Honolulu

Support for the continuation and expansion of the AFPM position has come from:

- The GAO: In his testimony, GAO International Affairs Director Jess Ford said that the GAO is "recommending that the State Department consider designating additional positions for fraud prevention" and that the DOS's decision to eliminate the AFPM's "didn't seem like it was a good idea to us". The GAO report found that fraud referral rates dropped "almost 25 percent" during the period when the AFPM's were eliminated.
- Former DS Special Agent in Charge Michael Johnson: In his testimony, Mr. Johnson stated that he told "various Consular Affairs officials that I really felt that [the elimination of the AFPM] was not a very good idea" because "many of these assistants had been in those jobs for years and years and years and had a great deal of local and national knowledge when it came to fraud". He asked, "why not leave the assistants there and then still rotate?"
- Former Senior Management Officials: The fact that the number of AFPM positions was greatly increased by HQ Management is the strongest possible indication of support for the position. After the GS-9 AFPM PD was supplanted by the GS-11 Specialist PD in1996, the number of AFPM's grew from 4 positions in 4 offices to 14 positions in 12 offices.
- Fraud Program Managers: The GAO talked in person or on the phone with all of the FPM's and the "fairly consistent message we heard was that the elimination of the [AFPM] was viewed as hurting the effort to look at fraud." At their 2002 conference, virtually all of the

FPM's expressed the importance of upgrading the AFPM position to a GS-11/12, and no one disagreed. The Union had often heard of discussions to upgrade the position to a GS-11/12, even to "piggyback" the AFPM upgrade onto the PD for a new Operations Officer position.

- Former Assistant Secretary of State Mary Ryan: On May 20, 1997, Assistant Secretary Ryan testified to the House Subcommittee on Immigration and Claims: "In addition to those sixteen full-time anti-fraud employees in CA/FPP, there is a fraud program manager in each of our fourteen passport agencies. Five of those have full-time assistants.... as evidenced by those numbers, combatting fraud is a priority for the Department."
- Teams of Current Management Officials From Many Offices: The Management Assessment and Internal Controls Review Reports involve teams of about six Management officials from regional offices and HQ reviewing the various functions of a single Passport Office. None of their reports recommended the elimination of any AFPM position. On the contrary, they have lauded the contributions of the AFPM's, requested additional resources for them, and observed that the position co-existed with GS-11's (and even GS-9's, 7's, and 5's) rotating through the FPM office. The 2003 review of Charleston stated that the FPM is "assisted fulltime by two contract clerical support staff and part time by two GS-11 Passport Specialists on a rotational basis. This is good but the office would benefit from a full time AFPM for continuity and back up", and suggested that even 2 AFPM's might be warranted. The 2003 Honolulu review stated, "a full-time assistant and clerical position for the fraud office are desperately needed" and "Strong consideration should be given to appointing a full-time Assistant Fraud Prevention Manager and a contract clerical staff person." An AFPM in Boston was hired after the 2001 review recommended it.
- Current Management Officials: the continuation of the AFPM position has received a great deal of "off-the record" support from other DOS Management personnel.
- Other DOS Bureaus and other Government Agencies: Staff at these agencies (BVS, DS, FPP, DMV, SSA) have expressed disappointed with the abolishment of the AFPM's.
- The Union: After canvassing the employees and Union officers in all offices, we issued a formal statement opposing the decision to eliminate the AFPM's. The Union unsuccessfully tried to address this in partnership meetings, formal bargaining, and with a grievance.
- Passport Services Employees: Coworkers of the AFPM's have nearly unanimously expressed the view that the position was a vital component of anti-fraud efforts.

The elimination of the permanent AFPM's has also resulted in increased costs to the taxpayers. The FPM's are probably away or unavailable at least 20% of the time, and now instead of paying a GS-11 AFPM to expertly fill in, the GS-11's rotating through to assist the FPM have to seek out the advice and guidance of other managers, including the GS-14 ARD and the GS-15 RD. The DOS is "in the process of adding more Fraud Prevention Managers [FPM] to the staffs in our larger agencies" but with second shifts, a second FPM in those offices was overdue already. We had heard that DOS was going to hire second FPM's for the fraud-heavy offices (New York, Miami, and Los Angeles) but this was not mentioned in the testimony.

There is a nexus between the AFPM position and other problems identified by the GAO. Problems with connectivity and communication between government agencies may only worsen as the AFPM's had established numerous contacts that allowed them to facilitate our anti-fraud efforts as well as assist those other offices (many of them law enforcement) in fulfilling their missions. The 2003 analysis of the workload transfer problem was possible because of a sophisticated database created by one of the AFPM's, who also created the Seattle online fraud library mentioned in the GAO's report. He was "reassigned" when his AFPM position was eliminated.

Insufficient fraud prevention oversight of Acceptance Agents

The final GAO recommendation for improving passport fraud detection capabilities is to strengthen training and oversight of the approximately 7000 passport acceptance agents, which include libraries, universities, post offices, county clerk offices, and neighborhood service centers. Most passport applicants have 100% of their face-to-face dealings in the passport process with these acceptance agents, whose job it is to verify the applicant's identity, administer the oath, execute the application, and forward it along with the subject's citizenship evidence to the contracted banking center to begin processing. The number of facilities has dramatically increased in the last 5 years, largely to meet the needs of increased numbers of passport applicants and because the DOS switched to an appointment-only system for expedited applications only at the Passport Agencies.

Some of the vulnerabilities in our system associated with utilizing acceptance agents include:

- Some acceptance agents have had not any training whatsoever, yet they can begin accepting applications as soon as they receive their appointment. Anecdotally, there have been instances where agents with 15 years of experience were consistently failing to follow procedures since they were unaware what the correct procedures were.
- Other agents have received little or infrequent training.
- Many agents are new to the assignment.
- As noted at the HSGAC hearing, the list of acceptance agents is continually outdated.
- Agents have split duties, such as selling stamps, receiving utility payments, and issuing permits, so that they may not be consistently assigned to the passport acceptance duty.
- Training packets and newsletters do not consistently reach all of our acceptance facilities. With 7000 facilities, the DOS is not able to follow up to check that updates to instructions are received, let alone understood.
- The screening process for acceptance agents is much less rigorous than that used by the DOS for its own employees. Some anecdotes:
    - At every training session she has given, on Passport Specialist asks if there are any non-citizens in attendance, and every time the answer is yes (they have to leave).
    - Another Specialist reported that in her training session, one acceptance agent volunteered that she was not a citizen, so she had to leave.
    - At that same session, two acceptance agents alleged to the Specialist that another agent at the training was a convicted felon who did not have the right to vote.
    - As pointed out in testimony before the HSGAC, one acceptance facility had to be dropped in 2004 because a corrupt county employee had been selling fraudulent birth certificates to illegal aliens
- The DOS does not have the resources to provide training or visit most of the facilities.
- The policy of allowing some applications to be executed at a facility and "hand-carried" by a courier service to the Passport Agency exposes our internal controls to others.
- Our current system of 7000 acceptance facilities effectively vetoes any possibility of including additional biometrics (fingerprints or retinal scans) into the U.S. passport.

The failure to properly follow correct execution procedures can thwart efforts by an Assistant U.S. Attorney to prosecute a passport fraud case. The Canadian Passport office has 30 offices for a population of 32 million, while the U.S. has 16 offices for almost 300 million. While it would be a very large undertaking, some consideration should be given to following the Canadian model.

Questions for the Record submitted to
Deputy Assistant Secretary Frank Moss by
Senator Susan M. Collins
Senate Committee on Homeland Security
and Governmental Operations
June 29, 2005

Question:

Your testimony describes your efforts to develop and deploy the new U.S. electronic passport with a contactless chip and enhanced security features. I understand that you have begun narrowing procurement options at least for an initial test phase of the program and that foreign companies have expressed the greatest interest in partnering with the U.S. on this program. Will you provide us with assurances that you will make sure that the truly best minds, whether they be foreign or domestic, are considered as you tackle these difficult technical and security issues?

Answer:

The Department of State and the U.S. Government Printing Office (GPO) have conducted a full and open competition that was open to all sources of expertise, both foreign and domestic, that could provide the desired components for the electronic passport. Prior to preparing our technical specifications, we initially solicited expertise in the field of contactless chip technology with the publication of a global Request for Information (RFI) regarding the technology. This RFI provided a wealth of information that assisted in preparing the content of our procurement request for electronic passport components. The experience of the prospective

vendor with the technical standards for the use of contactless technology established by the International Civil Aviation and the International Standard Organizations was also a considerable factor in the initial review of technical proposals for the electronic passport procurement. We are now in the final stages of testing and selection of the offered components of nine different foreign and domestic companies that provided materials to GPO under the solicitation. The testing, that includes evaluation of compatibility with GPO book production equipment and the current U.S. passport, also assesses the durability of the components as integrated into passports, and the security of the physical document design as well as the chip operating system.

We fully agree with your desire to secure the best minds possible to work with us on this project. To that end, we established a Memorandum of Agreement with the National Institute of Standards and Technology (NIST) to conduct testing and evaluation of the components for electronic passports in response to our full and open competition being conducted by GPO. We have also engaged NIST's Electro-Magnetics Division in Boulder, Colorado to provide expertise on the security and privacy issues related to the use of contactless chip technology. We believe that NIST provides both an impartial and expert body of scientists that can provide the expertise that you suggest.

We will continue to seek that advice of experts within the Government as we finalize the selection and design of the U.S. electronic passport.

Questions for the Record submitted to
Deputy Assistant Secretary Frank Moss by
Senator Joseph Lieberman (#1)
Senate Committee on Homeland Security
and Governmental Operations
June 29, 2005

Question:

The GAO Report reported that"[n]umerous passport-issuing agency officials and Diplomatic Security investigators told [GAO] that the acceptance agent problem is a significant fraud vulnerability . . . State has almost 7,000 passport acceptance agency offices, and none of the 16 issuing offices provide comprehensive annual training or oversight to all acceptance agency offices in their area." In addition to the lack of comprehensive oversight, the Department of State does not have a list of individuals authorized to accept passport applications; for example, officials at one passport issuing office told GAO that "while their region included more than 1,000 acceptance facilities, the office did not maintain records of the names of individuals accepting passport applications at those facilities and the office did not keep track of how many individuals acted in this capacity a those facilities."

Many of the passport-issuing agencies are at local post offices and other federal facilities while others are at county clerks' offices and other non-federal facilities. In October of 2004, the former deputy registrar of the Hudson County Office of Vital Statistics pleaded guilty to creating fake, backdated birth certificates that illegal. Immigrants used to apply for U.S. passports. She admitted that a single broker paid her for the multiple birth certificates and provided her with names, dates of birth and other information.

Question #1a.

Of the 7,000 passport acceptance agency offices, please identify how many are operated by federal entities and how many are operated by non-federal entities. Of the non-federal entities, please identify the different types of governmental and non-governmental entities that operate passport

acceptance agencies, and the numbers of acceptance agency offices that fall into each category.

Answer:

Currently, there are 7,462 active locations that accept applications for regular tourist passports from the general public. Of these, there are 4,318 federal entities, all of which are U.S. Post Offices, and 3,144 non-federal entities designated as passport acceptance facilities. Of the non-federal entities, the category and number for each type of acceptance facility is as follows:

Clerks of Court – 2,128

Municipal Offices – 585

County/State Offices – 327

Public Libraries – 83

Public Universities/Schools – 21

Diplomatic, Official and Military passports are issued by the Special Issuance Agency (SIA). SIA designates individuals as passport acceptance agents. Of these passport acceptance agents, 70 are at federal agencies and

1,801 are military passport acceptance agents who are stationed at military bases in the U.S. and abroad.

Question #1b:

What efforts, if any, does the State Department take to maintain up-to-date and comprehensive records of the names of individuals accepting passport applications at passport acceptance offices?

Answer:

At the time an entity applies to become a passport acceptance facility, the facility manager is required to submit the names and signatures of all persons to be assigned as passport acceptance agents.

It is the Department of State's directive that once designated as a passport acceptance facility, an entity is required to provide, on an annual basis, an updated list of names and signatures of individuals accepting passport applications at its facility. All passport acceptance facility designation records, including the names and signatures of acceptance agents, are kept and maintained by our Passport Agency Customer Service Managers, who manage and oversee the acceptance facility program located in their regions.

Questions for the Record submitted to
Deputy Assistant Secretary Frank Moss by
Senator Joseph Lieberman (#2)
Senate Committee on Homeland Security
and Governmental Operations
June 29, 2005

Question #2:

Passport acceptance agents are responsible for accepting passport applications and verifying that an applicant's identification document actually matches that applicant, who is required to be physically present. In the fraud case at the Hudson County Office of Vital Statistics, the corrupt county official issued multiple bogus backdated birth certificates to a middleman. The ultimate recipient of the fake documents was never present in the county office.

Question #2a:

Could a middleman arrange for corrupt employees at an acceptance facility to both issue a fake birth certificate and falsely attest to the identification of the applicant, when the applicant was in fact still in another country, thus allowing a watch listed terrorist to enter the United States under an assumed identity with a seemingly legitimate U.S. passport?

Answer:

Currently our national policy prevents an acceptance agent from performing the function of vital statistics issuance. This creates an environment where we eliminate one person from performing both functions, thereby reducing the ability of a middleman arranging for corrupt employees at an acceptance facility from issuing both a fake birth certificate

and falsely attesting to the identification of a passport applicant. As such, the possibility of your questioned scenario permitting a watch-listed terrorist from entering the U.S. under an assumed identity, with a legal passport, is also reduced.

Question #2b:

What fraud detection and oversight does the Department of State conduct, with respect to passport acceptance agents, to prevent a terrorist in another country from acquiring a U.S passport through corruption?

Answer:

The largest provider of passport acceptance services, the U.S. Postal Service (USPS), cooperated with us to develop and implement a computer-based (CBT) modular, interactive training program for Passport Acceptance Agents. The CBT includes training related to passport fraud and includes a test for each subject matter module, all of which must be passed in order for a postal employee to accept passport applications.

The Department of State is working with an educational contractor to adapt this training for non-postal Acceptance Agents. We are developing structured computerized registration, testing and recordkeeping for use by our national network of Passport Agencies for initial Acceptance Agent training.

Passport Agencies maintain an Acceptance Facility Database (AFD), which includes all relevant information for recordkeeping purposes. The Department is exploring modifying the database to expand its flexibility and usefulness for maintaining an inclusive, standardized electronic history that will include training, site visits, fraud identification, and quality assurance (audits) across geographic regions.

Passport Services now requires acceptance agents to enter a unique Acceptance Facility identification number for each passport application. In the next upgrade of its Travel Document Issuance System (TDIS), this number will allow the Department to track accepted passport applications by each facility, enabling us to identify what caused a facility's applications to be delayed due to missing information and/or inadequate documentation. In addition, senior Department managers will review all facets of the Acceptance Agent program to identify opportunities for additional fraud controls and oversight.

Acceptance facilities now must provide acceptance agent signature samples once a year for all agents. This helps to prevent unauthorized signature use. In addition, quality reviews will be conducted on passport applications and supporting documents from new acceptance facilities, as well as those with high fraud or error rates. Semi-annually, the Department

will also notify USPS and other acceptance facilities of the requirement that all acceptance agents must be US citizens, without criminal histories.

It is important to understand that passport acceptance agents can only accept passport applications. They do not have the authority or means to adjudicate or issue U.S. passports. All passport applications taken by acceptance agents must be submitted to a passport-issuing facility for review, processing, and adjudication.

The Department takes fraud detection and oversight very seriously. The aforementioned requirements have been instituted by the Department not only to prevent fraud, but also to give the Department feedback and oversight on the progress of our passport fraud prevention program. In this day of terrorist threats, the Department is taking measures to ensure not only that our borders are protected, but also that we put in place a fraud prevention structure that counters corruption of our passport process.